La protection de la vie privée dans l'e-gouvernement

Degrave, Élise

Published in:
Vie privée et données à caractère personnel

Publication date:
2015

Document Version
le PDF de l'éditeur

CHAPITRE 12.5.
LA PROTECTION DE LA VIE PRIVÉE DANS L'E-GOUVERNEMENT[1]

Élise DEGRAVE

I. La transformation de l'administration par les technologies

1. De l'administration en silos à l'administration en réseaux. Aujourd'hui, l'administration est engagée dans l'ère de l'*electronic government* ou « e-gouvernement », que l'on appelle aussi « administration électronique ». Ce terme générique désigne l'ensemble des utilisations des technologies de l'information et de la communication dans l'administration, ainsi que les mutations que ces utilisations y engendrent[2].

L'informatisation de l'administration n'est pas une simple modernisation de celle-ci. Le déploiement des technologies dans le secteur public n'aboutit pas seulement à remplacer les fichiers papier par des bases de données électroniques et à permettre

1. La présente contribution s'inspire de publications corollaires du même auteur : « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.,* 2009, pp. 365 à 371 ; « L'e-gouvernement et la protection de la vie privée », *C.D.P.K.,* 2013, pp. 53 à 64 ; « Transparence administrative et traitements de données à caractère personnel : note d'observations sous Cass. (1re ch.), 14 janvier 2013 », *R.D.T.I.,* 2013, pp. 53 à 64 ; *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* coll. CRIDS, Bruxelles, Larcier, 2014 ; « L'obligation de collecter les données à caractère personnel via la Banque-carrefour de la sécurité sociale : un renforcement de la responsabilité des institutions de sécurité sociale », *T.S.R.-R.D.S.*, 2014, pp. 525 à 557 ; « L'intégrateur de service fédéral au cœur de la simplification administrative », *A.P.,* 2014, pp. 518 à 536.
2. É. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 33. Voy. également les éléments les plus pertinents mentionnés dans différentes descriptions de l'e-gouvernement reprises dans les documents suivants : COMMISSION DES COMMUNAUTÉS EUROPÉENNES, « Le rôle de l'administration en ligne (eGovernment) pour l'avenir de l'Europe », *COM*(2003) 567 final, du 26 septembre 2003, p. 4 ; COMMISSION DES COMMUNAUTÉS EUROPÉENNES, « L'information émanant du secteur public : une ressource clef pour l'Europe. Livre vert sur l'information émanant du secteur public dans la société de l'information », *COM*(1998) 585, p. 8 ; OBSERVATOIRE DES DROITS DE L'INTERNET, « Facteurs de succès de l'e-gouvernement. Avis n° 2 », décembre 2003, disponible sur le site http://www.internet-observatory.be ; BANQUE MONDIALE, « Definition of E-Government », http://web.worldbank.org ; R. SILCOCK, « What is e-government ? », *Parliamentary Affairs,* 2001, vol. 54, p. 88 ; D. DE ROY, C. DE TERWANGNE et Y. POULLET, « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K.,* 2007, p. 310 ; E. BOUDRY, F. DE RYNCK, S. JANSSENS et S. ROTTHIER, *E-government : nieuwe kans of nieuw probleem,* Brugge, die Keure, 2009, pp. 1 et 2 ; G. CHATILLON, « Fondements, principes et nature du droit de l'administration électronique », *in* G. CHATILLON (dir.), *Droit de l'administration électronique. De nouveaux droits pour les usagers. Des nouvelles règles pour les agents*, Bruxelles, Bruylant, 2011, pp. 28 et 29 ; P. TRUDEL, « Existe-t-il un droit public de la gouvernance en ligne ? », *in ibid.,* p. 312 ; F. BUNDSHUCH-RIESENEDER, « Governance and e-governance in the frame of Bologna Process », *in* T. COME et G. ROUET (dir.), *Bologna Process, European Construction, European Neighbourhood Policy*, Bruxelles, Bruylant, 2011, p. 260.

l'envoi de courriels plutôt que de courriers postaux. L'administration est aujourd'hui profondément bouleversée par les technologies, dans son fonctionnement, mais également dans sa structure.

En effet, durant longtemps, l'administration était structurée en silos. Les institutions publiques œuvraient de manière cloisonnée, collectaient auprès des citoyens les informations dont elles avaient besoin pour l'exécution de leurs propres missions et ne les partageaient pas ensuite. Il en résultait une perte de temps et d'argent pour l'administration, qui devait contacter chaque personne pour chaque information nécessaire, attendre sa réponse, réclamer éventuellement des précisions. Le citoyen pâtissait également de cette situation, contraint de communiquer de multiples fois la même information aux institutions gérant un dossier à son sujet, d'effectuer des démarches administratives qui impliquaient d'identifier l'administration compétente, de se déplacer, de respecter des horaires stricts et de prendre patience dans les files d'attente.

Avec l'apparition de l'informatique, on constate que les administrations peuvent désormais collaborer efficacement. La volonté naît alors d'encourager les « synergies entre les divers services et niveaux des pouvoirs publics »[1], dans le but de simplifier les démarches et procédures administratives. L'informatique rend aisé et rapide l'échange des informations relatives aux citoyens. Cela permet notamment d'alléger les tâches administratives des citoyens, en automatisant l'octroi de certaines allocations par exemple, et de renforcer l'efficacité de l'administration, en améliorant la lutte contre la fraude notamment[2].

Pour mettre en œuvre efficacement l'échange des informations entre administrations, la Belgique s'engage, depuis plusieurs années, dans un modèle d'organisation administrative tout à fait inédit, qui consiste à mettre en place des réseaux d'administrations au sein desquels un intégrateur de services assure l'échange des données entre les administrations concernées.

Plus précisément, dans un premier temps, les administrations ayant un point commun (p. ex., un objet de travail commun ou l'appartenance à une même entité, fédérale ou fédérée) sont regroupées au sein d'un ensemble appelé « réseau ».

Ensuite, différentes administrations se voient attribuer la responsabilité de collecter, enregistrer et mettre à jour certaines données déterminées. Les bases de données contenant ces informations et placées chacune sous la responsabilité d'une administration sont appelées « sources authentiques de données ». L'idée est de faire en

1. Commission de la protection de la vie privée (ci-après, « CPVP »), avis n° 41/2008 du 17 décembre 2008 relatif à une demande d'avis concernant l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de services fédéral, n° 5.
2. Pour de plus amples développements sur l'e-gouvernement et le modèle de l'administration en réseaux, voy. D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen*, Brugge, Vanden Broele, 2005, pp. 1 à 13 ; É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, en particulier n^os^ 172 et s. Voy. *infra,* n° 3.

sorte que chaque information relative au citoyen ne soit enregistrée qu'une seule fois par une seule administration du réseau, qui est ensuite responsable de la fiabilité de ces données.

Enfin, on place, au cœur de ce réseau d'administrations, un outil d'un type nouveau : l'intégrateur de services, dit aussi « plateforme d'échange d'informations » ou encore « banque-carrefour ». En somme, l'intégrateur de services est une infrastructure technique, placée au cœur d'un réseau d'administrations et qui est chargée d'assurer, au sein de ce réseau, l'échange électronique d'informations provenant de sources authentiques diverses. Ainsi, lorsqu'une administration a besoin d'une donnée dont elle ne dispose pas, il lui suffit de s'adresser à l'intégrateur de services qui contacte l'administration détentrice de la donnée recherchée et l'achemine ensuite vers l'administration qui la lui a demandée.

Afin de faciliter la compréhension de l'exposé, on peut, d'ores et déjà, schématiser comme suit le modèle d'un réseau d'administrations comprenant un intégrateur de services.

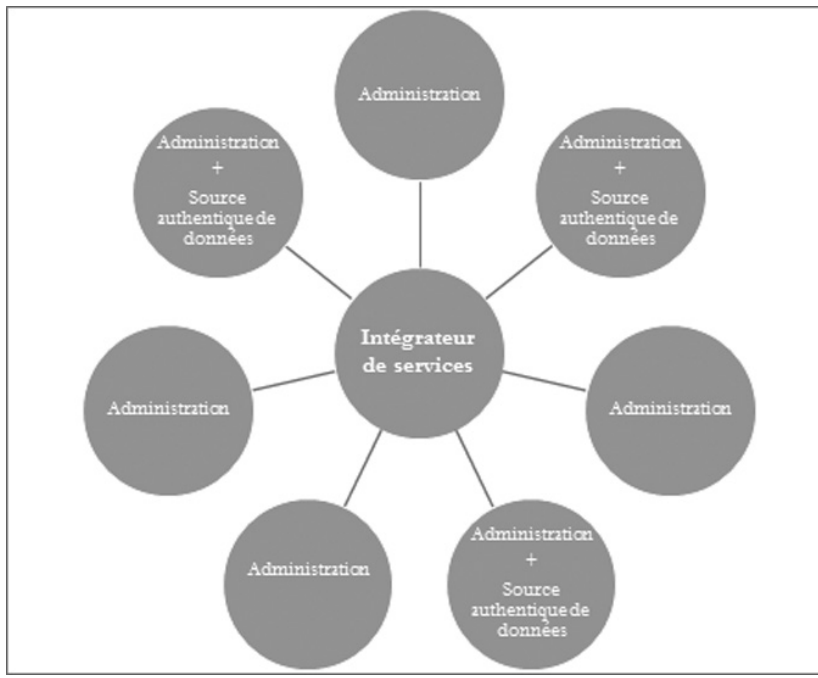
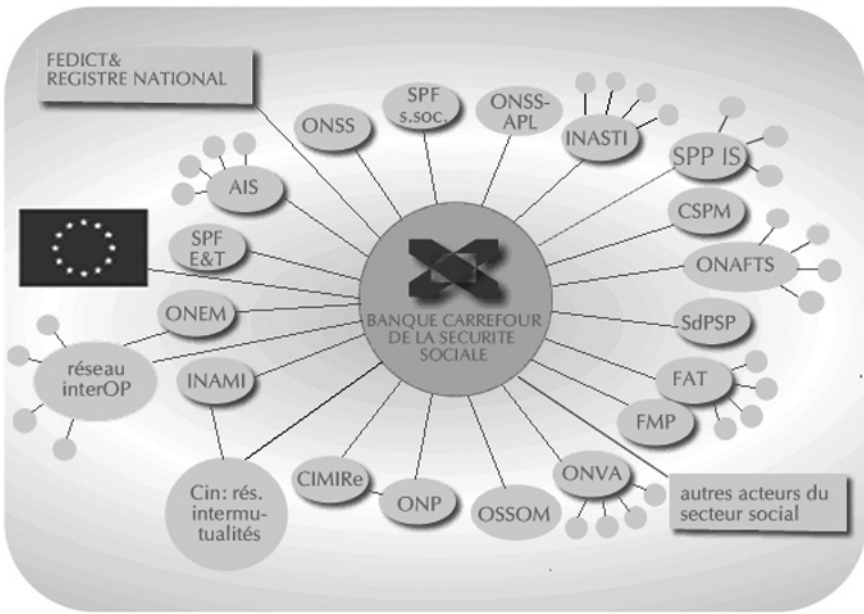


Schéma illustrant un réseau d'administrations composé d'un intégrateur de services auquel sont reliées plusieurs administrations dont certaines détiennent une source authentique de données.

2. Plusieurs réseaux d'administrations et intégrateurs de services. Depuis quelques années, plusieurs réseaux d'administrations ont progressivement été créés au sein du secteur public belge. Ils comprennent chacun, en leur cœur, un intégrateur de services.

Les premiers réseaux créés sont des réseaux dits « sectoriels », car ils sont liés à un domaine particulier de l'administration. L'intégrateur de services placé au cœur de ces réseaux sectoriels est qualifié d'intégrateur « vertical » par opposition aux intégrateurs de services « horizontaux » décrits ci-après. Le premier réseau du genre est le réseau de la sécurité sociale, qui regroupe les institutions de sécurité sociale et au sein duquel œuvre la Banque-carrefour de la sécurité sociale. Ce réseau et cet intégrateur de services sont en place depuis le début des années 1990[1]. A suivi la création, en 2008, du réseau sectoriel de la santé, au sein duquel la plate-forme *eHealth* assume le rôle d'intégrateur de services[2].



Exemple d'intégrateur de services vertical : la Banque-carrefour de la sécurité sociale, placée au cœur du réseau de la sécurité sociale[3]

1. Voy. la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.,* 22 février 1990 (ci-après, « loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale »).
2. Voy. la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme *eHealth* et portant diverses dispositions, *M.B.,* 13 octobre 2008.
3. Le schéma provient du site http://www.http://iis.bcss.fgov.be/Fr/missions/missions_3.htm.

Bien que ce modèle soit séduisant, la multiplication d'intégrateurs de services verticaux présente une difficulté particulière, à savoir que les administrations qui ont besoin d'informations relatives à un citoyen dont elles gèrent le dossier sont contraintes de s'adresser à différents intégrateurs de services en fonction du type de donnée recherchée. Or ces derniers ont chacun leurs outils spécifiques et leurs procédures particulières.

Dès lors, dans un deuxième temps et depuis peu, des réseaux et intégrateurs de services dits « horizontaux » ou encore « transversaux » sont mis en place. Ces réseaux regroupent des administrations en fonction de leur appartenance à l'entité fédérale ou à une entité fédérée. Ils contiennent un intégrateur de services chargé d'assurer la circulation des données entre les administrations concernées. Ainsi, en 2012, est créé l'intégrateur de services fédéral, qui sera étudié dans les lignes qui suivent. Au niveau des entités fédérées, l'intégrateur de services flamand est créé en 2012 pour assurer l'échange électronique des données au sein du réseau flamand constitué des institutions de la Communauté flamande et de la Région flamande[1]. Il s'agit du « Coördinatiecel Vlaams e-government » (CORVE). Les administrations de la Communauté française et de la Région wallonne sont également regroupées au sein d'un réseau au sein duquel œuvre, depuis 2013[2], un intégrateur de services, dénommé « Banque-carrefour d'échange de données » (BCED). Grâce à ces intégrateurs horizontaux, les administrations peuvent s'adresser à l'intégrateur de services de l'entité dont elles font partie (État fédéral, Communauté française et Région wallonne, Communauté flamande et Région flamande), sans devoir s'interroger sur le type de données recherché pour identifier leur interlocuteur. L'intégrateur se charge ensuite d'acheminer l'information recherchée vers l'administration qui l'a demandée, au besoin en contactant lui-même les intégrateurs de services verticaux que sont la Banque-carrefour de la sécurité sociale et la plate-forme *eHealth*.

3. Des avantages. De toute évidence, l'efficacité de l'administration est renforcée grâce à l'échange rapide d'informations exactes et à jour. En outre, puisque ces données sont disponibles sous forme électronique, on peut les réutiliser et y appliquer différents traitements. C'est ce que l'on fait notamment pour contrôler plus efficacement les citoyens. Par exemple, progressivement, se mettent en place des outils de profilage, pour lutter contre la fraude fiscale et sociale. Il s'agit de regrouper des données très différentes au sein d'une grande base de données appelée « entrepôt de données » ou *datawarehouse* et d'y appliquer des calculs très puissants appelés « algorithmes de fraude », basés notamment sur des calculs statistiques. Ce faisant, l'ordinateur peut identifier des personnes suspectées de fraude. Ces outils semblent très efficaces, puisque, selon les dires d'inspecteurs sociaux, jusqu'à présent, la plu-

1. Décret du 13 juillet 2012 portant création et organisation d'un intégrateur de services flamand, *M.B.,* 1er août 2012.
2. Décret du 4 juillet 2013 portant assentiment de l'accord de coopération entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.,* 23 juillet 2013.

part des personnes suspectées de fraude se sont révélées, après contrôle, être effectivement coupables de fraude[1].

Le citoyen voit également ses tâches facilitées. Il peut accéder à nombre d'informations en ligne et effectuer des transactions administratives à tout moment depuis son ordinateur. Il est également épargné de certaines démarches administratives grâce à l'automatisation des procédures. À cet égard, par exemple, une application informatique créée par l'intégrateur de services fédéral et dénommée *Ebirth* facilite l'échange des données relatives à la naissance d'un enfant. Ce service part du constat que tant les communes que la Communauté française et le SPF Économie ont besoin d'informations relatives à chaque naissance. Jadis, ces administrations obtenaient ces informations via des formulaires en papier envoyés par les hôpitaux. Aujourd'hui, les hôpitaux se connectent au portail *Ebirth*, encodent les données requises, et celles-ci sont acheminées respectivement vers les communes, la Communauté française et le SPF Économie[2].

4. Des dangers. De toute évidence, l'e-gouvernement est donc séduisant. Mais il est aussi dangereux. En général, lorsqu'on évoque le danger d'utiliser les technologies dans l'administration, on songe au spectre de *Big Brother.* C'est l'idée d'un État omniscient, qui saurait tout de tout le monde et pourrait surveiller chaque individu. Cette crainte est justifiée. Mais il existe également un autre danger tout aussi fondamental, plus rarement mis en évidence : celui de créer progressivement une administration kafkaïenne[3], c'est-à-dire une administration à ce point technique et complexe, à ce point distante, qu'elle en deviendrait incompréhensible et, dès lors, incontrôlable.

Face à ce constat, comment faire en sorte que, dans l'e-gouvernement, le citoyen ne soit pas exclu de cette évolution technologique et qu'il puisse continuer à comprendre et contrôler l'action de l'administration ? La réponse à cette question en appelle au droit à la protection de la vie privée et au droit administratif.

1. Pour de plus amples précisions sur la technique du profilage, voy. Recommandation CM/Rec(2010)13 du Comité des ministres du Conseil de l'Europe aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, disponible sur le site www.coe.int ; M. HILDEBRANDT, « Who is profiling who ? Invisible visibility », *in* S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE et S. NOUWT (éd.), *Reinventing Data Protection ?*, Dordrecht, Springer, 2009, p. 241 ; V. PAPAKONSTANTINOU, « A data protection approach to data matching operations among public bodies », *International Journal of Law and Information Technology,* 2001, vol. 9, n° 1, pp. 62 et 63 ; J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, « L'application de la Convention 108 au mécanisme de profilage. Éléments de réflexion destinés au travail futur du Comité consultatif », mars 2008, T-PD, (2008), 01, p. 5 ; É. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.,* n^{os} 40 et s.
2. Pour plus d'informations sur *Ebirth,* voy. la présentation générale d'*Ebirth* disponible à l'adresse https://www.ehealth.fgov.be/fr/services-en-ligne/ebirth/presentation-d-ebirth.
3. D. SOLOVE, « I've got nothing to hide' and other misunderstandings of privacy », *San Diego Law Review,* 2007, vol. 44, 745, 2007, pp. 745 à 772.

II. L'e-gouvernement aux confins du droit à la protection de la vie privée et du droit administratif

5. Le cadre juridique de l'e-gouvernement. Un enjeu fondamental sous-tend le développement de l'e-gouvernement : organiser un e-gouvernement efficace tout en octroyant au citoyen les moyens nécessaires pour garder une prise sur l'administration, afin de la comprendre et de la contrôler. De cette manière, l'efficacité de l'administration est encouragée, et le droit à la vie privée des individus est protégé.

Pour atteindre ce double objectif, un cadre juridique doit être créé pour l'e-gouvernement. Il doit être cohérent et adapté aux dangers de l'informatisation de l'administration.

Actuellement, l'e-gouvernement est soumis à un double régime juridique.

D'une part, le régime juridique de la protection de la vie privée et des données à caractère personnel doit être respecté, puisque le fonctionnement de l'e-gouvernement est fondé en grande partie sur le traitement informatisé des données à caractère personnel des citoyens. Le droit à la vie privée s'entend aujourd'hui du droit à l'autodétermination informationnelle[1]. Concrètement, cela signifie que chacun a le droit d'être conscient du fait que ses données circulent et sont traitées, de vérifier si elles sont exactes, de contester les abus dans l'utilisation des données et d'obtenir réparation du dommage éventuellement subi à la suite de ces abus. Il y a donc lieu de mettre en place les moyens nécessaires pour garantir au citoyen la satisfaction de telles prérogatives dans l'e-gouvernement.

D'autre part, bien que l'administration se modernise considérablement, les règles de droit administratif général restent d'application. Or, ces vieilles règles, applicables depuis toujours à l'administration, ont été pensées en dehors de toute préoccupation liée aux technologies. Elles doivent aujourd'hui recevoir une interprétation nouvelle, adaptée aux enjeux de l'e-gouvernement.

Ainsi, pour organiser un cadre juridique cohérent pour l'e-gouvernement, il s'impose de réfléchir à l'articulation entre le régime juridique de la protection de la vie privée et des données à caractère personnel et le droit administratif. Ce n'est pas une tâche aisée, puisque ces deux corps de règles sont fort distincts. De plus, de manière générale, la littérature scientifique consacrée à l'e-gouvernement est maigre. Les administrativistes délaissent bien souvent les questions de droit administratif soulevées par les technologies, comme s'ils craignaient les ordinateurs. Le même constat

1. Voy. notamment Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in* K. BENYEKHLEF et P. TRUDEL (dir.), *État de droit et virtualité*, Montréal, Thémis, 2009, pp. 169 et s.

vaut pour les spécialistes de la protection des données, qui semblent peu à l'aise dans les méandres du droit administratif. Pourtant, ces deux mondes peuvent dialoguer et apporter une réponse aux questions soulevées par l'e-gouvernement.

6. La légalité, la transparence et le contrôle de l'e-gouvernement. La légalité, la transparence et le contrôle de l'administration sont trois exigences qui fondent l'État de droit. Ces trois exigences fondamentales sont particulièrement ébranlées par l'e-gouvernement tel qu'il se développe actuellement. Partant de ce constat, des solutions doivent être dégagées, qui assurent le respect de ces exigences dans le contexte de l'e-gouvernement. Ces solutions se nourrissent tant du régime juridique de la protection des données à caractère personnel que du droit constitutionnel et du droit administratif généraux.

La légalité, la transparence et le contrôle de l'e-gouvernement sont analysés dans les lignes qui suivent.

III. La légalité de l'e-gouvernement

7. Comment le législateur doit-il encadrer l'e-gouvernement ? Les outils de traitement de données sont des ingérences dans la vie privée des citoyens. En vertu de l'exigence de légalité imposée par l'article 8 de la Convention européenne des droits de l'homme (CEDH) et l'article 22 de la Constitution, ces outils doivent être encadrés par une loi[1].

Deux raisons justifient l'intervention du législateur.

D'une part, l'exigence de légalité doit conduire à soumettre au débat démocratique l'organisation d'ingérences dans la vie privée des citoyens[2]. En particulier, il importe de veiller à ce que les traitements de données à caractère personnel effectués dans l'administration incarnent un juste équilibre entre l'efficacité administrative et la pro-

1. J. Vande Lanotte et G. Goedertier, *Handboek Belgisch Publiekrecht*, Brugge, die Keure, 2010, pp. 448 et 449, n° 688 ; P. De Hert, « Artikel 8. Recht op privacy », *in* J. Vande Lanotte et Y. Haeck (dir.), *Handboek EVRM, Deel 2. Artikelsgewijze commentaar*, Anvers, Intersentia, 2004, pp. 716 à 718 ; M. Melchior et C. Courtoy, *op. cit.,* p. 284 ; É. Degrave, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.,* 2009, pp. 368 à 370.
2. Le Cour constitutionnelle et la section de législation du Conseil d'État l'ont rappelé à plusieurs reprises. Voy. avis L. 37.765/1/2/3/4 du 4 novembre 2004 sur un avant-projet de loi-programme, *Doc. parl.,* Chambre, 2004-2005, n° 1437 ; avis L. 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. parl.*, Chambre, 2004-2005, n^{os} 1598/1 et 1599/1, cités par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'État. Chronique de jurisprudence – 2004 », *R.B.D.C.*, 2005/2, p. 260, n° 6 ; C.C., 21 décembre 2004, n° 202/2004, B.4.3 et B.6.3 ; C.C., 26 juin 2008, n° 95/2008, B.42 ; C.C., 18 mars 2010, n° 29/2010, B.16.1 ; C.C., 14 février 2013, n° 6/2013, B.5.7 ; C.C., 16 mai 2013, n° 66/2013, B.11.1.

tection de la vie privée des citoyens. Ce travail doit être effectué par le législateur. Si l'organisation de traitements de données était laissée exclusivement à la discrétion des administrations, celles-ci pourraient avoir tendance à apprécier la nécessité de tels traitements principalement au regard de leur intérêt immédiat, celui de l'efficacité administrative, et à donner trop peu de poids à la protection de la vie privée des citoyens.

D'autre part, la loi doit être accessible et prévisible. De cette manière, les citoyens peuvent prendre connaissance des ingérences organisées dans leur vie privée. L'accessibilité et la lisibilité des textes organisant des ingérences dans la vie privée importent particulièrement lorsqu'il est question de traitements de données à caractère personnel. En effet, l'utilisation d'informations personnelles fait peur aux citoyens, car les outils nouveaux de traitements de données paraissent complexes et opaques. Les personnes concernées craignent également que l'objectif poursuivi lors de la collecte de leurs informations soit détourné et se retourne finalement contre elles. L'exigence de prévisibilité de la norme prend dès lors tout son sens pour établir la confiance entre les citoyens et l'État qui met en place de tels outils.

8. Des lacunes législatives. Pour l'heure, on constate que des aspects importants de l'e-gouvernement ne sont malheureusement pas organisés par le législateur. Par ailleurs, lorsqu'elles existent, les lois qui encadrent l'e-gouvernement ne répondent pas pleinement à cette exigence de légalité. L'e-gouvernement est ainsi soumis à des normes multiples, éparses et, dès lors, difficilement accessibles. Celles-ci sont également peu compréhensibles, tant le jargon lié à l'e-gouvernement est technique et complexe. Enfin, certaines lois prennent la forme de loi « fourre-tout », ou de « loi-programme », si bien que les traitements de données ainsi organisés n'ont pas fait l'objet d'un réel débat démocratique.

Face à ce constat, comment le législateur doit-il encadrer l'e-gouvernement pour répondre, d'une part, à l'exigence constitutionnelle de légalité, tout en tenant compte, d'autre part, des contraintes de l'e-gouvernement qui s'opposent à une interprétation trop stricte de cette exigence constitutionnelle ? Plus précisément, à quels critères le législateur peut-il se référer pour encadrer au mieux les traitements de données dans l'administration ?

9. Définir les éléments essentiels du traitement de données. L'analyse des arrêts de la Cour constitutionnelle et des avis de la section de législation du Conseil d'État rendus en la matière révèle que le législateur doit définir lui-même les éléments essentiels d'un traitement de données à caractère personnel. Il s'agit, par exemple, du type de données enregistrées dans une base de données, des institutions qui peuvent accéder à ces informations, de la durée d'enregistrement de ces données, etc. Le rôle du législateur est donc ample. Cela a des conséquences sur le rôle du Roi qui, sans être réduit à néant, est néanmoins fortement diminué dans l'e-gouvernement.

Il n'en demeure pas moins que, malgré la mise en lumière des éléments essentiels du traitement, la tâche du législateur demeure assez floue. Par exemple, comment déterminer les données qui doivent figurer dans une base de données ? Comment choisir entre un numéro d'identification unique ou un numéro d'identification sectoriel ? À quelles conditions peut-on mettre en place un *datawarehouse* pour lutter contre la fraude fiscale et sociale ? Le législateur doit être guidé dans de tels choix. Le régime juridique de la protection des données à caractère personnel l'y aide, en organisant une exigence de finalité et une exigence de proportionnalité.

On constate que le régime juridique de la protection des données à caractère personnel, s'il est correctement appliqué, offre au législateur des critères qui lui permettent de mieux légiférer. Ainsi, d'une part, le traitement de données doit poursuivre une finalité légitime, déterminée et explicite. D'autre part, le critère de proportionnalité impose un examen minutieux du caractère nécessaire et approprié du traitement mis en place et des données utilisées. Malheureusement, ces critères sont assez flous et posent de nombreuses questions en pratique. Il en va d'autant plus ainsi que peu de doctrine et peu de jurisprudence aident à comprendre la manière de les appliquer dans le secteur public. Ces critères doivent être interprétés, en s'inspirant notamment des nombreux avis rendus par la Commission de la protection de la vie privée (CPVP). On les analyse dans les lignes qui suivent, en se concentrant sur deux critères particulièrement importants : le critère de finalité et le critère de proportionnalité.

A. Le critère de finalité

10. La notion. La finalité d'un traitement de données est l'objectif en vue duquel il est réalisé.

Le cumul de l'article 8 de la CEDH et de la directive 95/46 aboutit à exiger que la finalité d'un traitement soit légitime, déterminée et explicite.

La finalité constitue « l'axe focal »[1] d'un traitement de données, puisqu'elle impose « le cadre dans lequel les diverses opérations de traitement peuvent avoir lieu »[2]. *In fine,* elle doit permettre « d'apprécier facilement et valablement la pertinence et la proportionnalité des données collectées »[3].

1. CPVP, avis n° 24/96 du 13 septembre 1996 relatif à la consultation des dossiers de la Police des étrangers déposés aux Archives générales du Royaume, p. 5 ; CPVP, avis n° 32/2001 du 10 septembre 2001 relatif à l'organisation de la publicité cadastrale, p. 3. Sur l'importance de l'exigence de finalité compte tenu de sa fonction d'encadrement des traitements de données, voy. également la thèse de R. Duaso Calès, *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau*, Université de Montréal et Université Panthéon-Assas Paris II, septembre 2011, pp. 14 à 19.
2. CPVP, avis n° 11/2007 du 31 mars 2007 relatif à un avant-projet de loi réglant l'application automatique des prix maximaux pour la fourniture d'électricité et de gaz naturel aux clients protégés résidentiels à revenus modestes ou à situation précaire, p. 3, n° 7.
3. CPVP, avis n° 14/2006 du 24 mai 2006 relatif au projet d'arrêté royal déterminant les règles suivant lesquelles certaines données hospitalières doivent être communiquées au ministre qui a la Santé publique dans ses attributions, p. 6, n° 27.

11. La raison d'être. L'attention portée à cette exigence s'explique par les risques induits lorsqu'elle n'est pas respectée. En effet, les dangers pour la protection de la vie privée des citoyens naissent davantage de l'utilisation faite de leurs données que de la nature de celles-ci. Des informations *a priori* banales peuvent ainsi causer préjudice aux personnes concernées si elles sont utilisées dans un but illégitime[1]. Par exemple, les dates de congé d'un fonctionnaire pourraient nuire à celui-ci si elles sont utilisées pour apprécier le droit à une promotion[2]. Le registre de la DIV, contenant notamment la plaque d'immatriculation des conducteurs et leur numéro de téléphone, peut être la source de harcèlement téléphonique de jolies conductrices dont le numéro de plaque aurait été noté par un policier ayant accès à ce registre. Un fonctionnaire communal organisé et prévoyant pourrait utiliser la date de naissance des citoyens, enregistrée au Registre national, pour contacter ceux-ci le jour de leurs 70 ans afin de leur demander s'ils souhaitent réserver une concession de sépulture dans la commune. Ces situations malencontreuses illustrent l'importance du travail du législateur à qui il revient d'identifier, le plus minutieusement possible, le but poursuivi par chaque collecte de données effectuée par une administration et de consacrer cette finalité dans la loi, de manière à cadenasser l'utilisation de telles informations. C'est d'autant plus important que, rappelons-le, les citoyens sont contraints de fournir leurs données aux administrations.

L'exigence de finalité impose au législateur de déterminer l'objectif du traitement d'une manière assez précise. Il ne peut se contenter d'affirmer, par exemple, que le traitement de données doit correspondre aux missions de l'administration. Des indications plus fines doivent être fixées. Dès lors, grâce à l'exigence de finalité requise par le régime juridique de la protection des données, le législateur est en mesure de baliser, de manière assez serrée, l'action de l'administration. C'est pourquoi les règles de protection des données constituent une voie intéressante pour permettre au législateur de baliser l'action de l'administration.

Ainsi qu'on l'a dit, la finalité poursuivie doit être légitime, déterminée et explicite. Ces exigences sont analysées à présent.

12. Une finalité légitime. L'article 8, § 2, de la CEDH prévoit que l'ingérence d'une autorité publique dans le droit à la protection de la vie privée doit constituer « une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à

1. Rapport fait au nom de la Commission de la Justice par M^me^ Mercks-Van Goey concernant le projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la proposition de loi relative à la protection de données personnelles concernant les personnes physiques dans les fichiers informatiques ou banques de données et à la création d'une commission nationale de l'informatique et des libertés, *Doc. parl.,* Chambre, S.E. 1991-1992, n° 413/12, p. 87 ; H. BURKERT, « The dimensions of information law », *in La télématique,* t. I, Gand, Story-Scientia, 1984, p. 217 ; Y. POULLET, « L'informatique menace-t-elle nos libertés ? », *in ibid.,* p. 195 ; M.-H. BOULANGER, C. DE TERWANGNE et T. LÉONARD, « La protection de la vie privée à l'égard des traitements de données à caractère personnel – La loi du 8 décembre 1992 », *J.T.,* 1993, p. 377 ; B. DOCQUIR, « Le droit de la vie privée : aperçu général et règle de proportionnalité », *in* B. DOCQUIR et A. PUTTEMANS (dir.), *Actualités du droit de la vie privée*, Bruxelles, Bruylant, 2008, pp. 32 et 33.
2. CPVP, avis n° 06/97 du 19 février 1997 sur l'utilisation de données concernant les jours de maladie et évaluation de données relatives à la santé dans le cadre d'une procédure de promotion au sein du ministère des Finances.

la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ». La directive 95/46 donne écho à ces valeurs, en affirmant que « les systèmes de traitement de données sont au service de l'homme ; ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus »[1].

Des dérogations au droit au respect de la vie privée sont donc admises. Il ne peut en être autrement, car le fonctionnement d'un État ne peut se passer de certaines ingérences dans ce droit fondamental lorsqu'elles sont motivées par le souci de satisfaire des objectifs légitimes dans une démocratie. C'est pourquoi, par exemple, la Commission de la protection de la vie privée[2] a considéré que le contrôle et la maîtrise des dépenses d'assurance maladie en matière de soins de santé représentent « une finalité légitime justifiant la transmission par les organismes et établissements dispensant des […] prestations remboursables par l'assurance maladie à des assurés sociaux ou à leurs ayants droit », car une telle finalité vise à protéger « le bien-être économique du pays »[3].

Les valeurs affirmées par la Convention européenne des droits de l'homme, dans la lignée desquelles s'inscrit la directive 95/46, sont interprétées largement par la Cour européenne des droits de l'homme[4]. Celle-ci n'a d'ailleurs « jamais censuré une mesure étatique restrictive de liberté au motif que celle-ci ne poursuivrait pas l'un des buts légitimes énumérés » à l'article 8, § 2[5]. Il y a donc peu de risque qu'un traitement de données soit invalidé au motif qu'il viole une de ces valeurs.

C'est la raison pour laquelle la finalité d'un traitement ne peut se réduire à son assimilation à une valeur défendue par la Convention et qu'il importe d'en vérifier le caractère déterminé et explicite.

13. Une finalité déterminée. L'article 8, § 2, de la CEDH exige que l'ingérence dans le droit à la vie privée soit prévue par une loi. Selon la Cour européenne des droits de l'homme, cette loi doit être rédigée de manière telle que tout individu puisse « en prévoir les conséquences pour lui »[6]. Les normes organisant la protection des données

1. Considérant 3 de la directive 95/46 précitée.
2. Ci-après, « CPVP ».
3. CPVP, avis n° 12/2002 du 21 mars 2002 relatif à un projet d'arrêté royal fixant les règles suivant lesquelles certaines données statistiques minimales psychiatriques doivent être communiquées au ministre qui a la Santé publique dans ses attributions, p. 5, n° 11. Dans le même sens, voy. l'avis n° 10/2008, du 27 février 2008, concernant une proposition de loi relative aux certificats de bonne conduite, vie et mœurs, p. 6, n° 28.
4. V. Coussirat-Coustere, « Article 8 § 1 », *in* L.E. Pettiti, E. Decaux et P.-H. Imbert (dir.), *La Convention européenne des droits de l'homme. Commentaire article par article*, 2e éd., Paris, Economica, 1999, p. 336.
5. Rapport de H. Claes et J.-J. Viseur fait au nom du groupe de travail chargé de l'examen du Titre II de la Constitution sur les clauses transversales en matière de droits et de libertés (experts : J. Velaers et S. Van Drooghenbroeck), *Doc. parl.,* Chambre, 2004-2005, n° 81-2304/001, pp. 21 et 22.
6. CEDH, arrêt *Leander c. Suède*, 26 mars 1987, § 50.

à caractère personnel traduisent cet impératif par l'obligation que tout traitement poursuive une finalité déterminée. Cette exigence n'est pas inconnue du législateur ni de l'administration. En effet, traditionnellement, en droit administratif, les administrations sont tenues au respect du principe de spécialité. Celui-ci veut que les institutions n'accomplissent que les missions qui leur ont été dévolues et les avis de la CPVP livrent des indices aidant le législateur à atteindre la précision requise lors de la définition d'une finalité.

a) Exclusion des critères imprécis. Tout d'abord, le législateur ne peut se contenter de prévoir que la finalité doit entrer *dans les missions* de l'administration concernée.

Par exemple, une source authentique de données ne peut être créée dans le seul but de permettre « l'exécution de diverses "tâches de service public" »[1] des administrations ou l'accomplissement de la « mission générale du service de gestion »[2] de cette banque de données. Prévoir qu'une administration a accès au Registre national « pour l'exécution de ses missions d'intérêt général » est également une formulation trop imprécise[3].

Dans le même sens, une finalité ne peut être définie à ce point largement qu'elle permette *tous les traitements* effectués par l'instance concernée. Ainsi, « la communication interne et externe requise par le fonctionnement de la justice » n'est pas une finalité suffisamment précise pour permettre le traitement de données à caractère personnel au sein du système d'information « Phénix ». En effet, selon la CPVP, « cette mention est peu spécifique et couvre toutes les applications tant d'une administration que d'une entreprise »[4]. Dans le même sens, la CPVP s'est prononcée sur l'enregistrement, par les hôpitaux, du résumé hospitalier minimal et des données « service mobile d'urgence », destinés à être transmis au ministre de la Santé publique. Elle a estimé que les finalités décrites n'étaient pas suffisamment précises, puisqu'elles légitiment « le traitement de quasiment toutes les données enregistrées dans un hôpital »[5].

1. CPVP, avis n° 42/2006 du 18 octobre 2006 concernant l'avant-projet de loi portant création d'une source authentique des données relatives aux véhicules, p. 6, n° 19.
2. CPVP, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi portant création de la source authentique des données relatives aux véhicules, p. 20, n° 57.
3. CPVP, avis n° 19/2002 du 10 juin 2002 concernant le projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, p. 7, n° 11. Dans le même sens, à propos de l'utilisation de la notion de « tâches liées à la gestion administrative » pour définir une finalité, voy. CPVP, avis n° 29/95 du 27 octobre 1995 relatif au projet d'arrêté royal autorisant l'accès au Fonds national de la recherche scientifique aux informations du Registre national des personnes physiques, p. 4, n° 6 ; l'avis n° 10/96 du 15 mai 1996 relatif au projet d'arrêté royal autorisant le Fonds du logement des familles nombreuses de Wallonie à accéder au Registre national des personnes physiques et à en utiliser le numéro d'identification, p. 4, et l'avis n° 11/96 du 15 mai 1996 relatif au projet d'arrêté royal autorisant la Société régionale wallonne du logement et les sociétés immobilières de service public agréées par celle-ci à accéder au Registre national des personnes physiques et à en utiliser le numéro d'identification, p. 6.
4. CPVP, avis n° 11/2004 du 4 octobre 2004 relatif à deux avant-projets de loi instituant la banque de données-Phénix, n^{os} 8 et 10.
5. CPVP, avis n° 14/2006 du 24 mai 2006, *op. cit.*, n° 27.

b) Fin en soi. En outre, la CPVP a soutenu que la finalité doit constituer une fin en soi, et non simplement un moyen d'atteindre cette fin[1].

On peut raisonnablement supposer que cette exigence s'explique du fait qu'un même moyen pourrait servir diverses finalités, qui n'entreraient pas toutes nécessairement dans les compétences légalement définies du responsable du traitement.

Ainsi, on ne peut admettre l'enregistrement, par une administration, de données relatives au véhicule des individus dans le seul but d'en « connaître le kilométrage ». En effet, ce dernier élément n'est qu'un moyen de réaliser un objectif final qu'il y a lieu de déterminer, à savoir, en l'occurrence, la protection des consommateurs contre la fraude relative au kilométrage[2].

Dans le même sens, on ne peut assigner comme finalité à une banque de données celle de « recueillir et [de] centraliser les informations sur l'état de l'emploi dans le secteur public de la Région [Bruxelles-Capitale] »[3]. Il y a lieu de définir le but poursuivi par ce traitement, qui ne peut être que celui d'« établir des statistiques anonymes pour soutenir la politique dans un certain nombre de domaines à préciser »[4].

Cette position est également confirmée en ce qui concerne les missions de la Banque-carrefour des entreprises. Plutôt que de dire que cette source authentique est chargée « de la récolte, du stockage et de la gestion des données portant sur l'identification des titulaires d'une inscription », il est préférable de préciser qu'elle assure « l'enregistrement, la mémorisation et la communication d'informations permettant l'identification des entreprises et la localisation des dossiers relatives à ces entreprises dans les diverses administrations, et ce, afin de faciliter les relations entre administrations et administrés et la fiabilité des échanges entre administrations »[5].

c) Critère fonctionnel. Pour constituer une fin en soi, la finalité doit être décrite à l'aide d'un critère fonctionnel, et non un critère organique. En d'autres termes, il ne faut pas seulement se demander à qui le traitement de données à caractère personnel doit servir (critère organique), mais bien *pour quelle(s) raison(s)* telle administration veut effectuer de tels traitements (critère fonctionnel).

---

1. Ce raisonnement de la CPVP a été utilisé pour critiquer une décision du comité sectoriel Registre national qui autorisait l'accès de Fedict au Registre national en vue de « tester, corriger et entretenir des applications informatiques qui ont une connexion avec le registre national via l'U.M.E., le F.S.B. et les webservices ». Voy. Y. POULLET, « Quelques réflexions à propos de la délibération n° 19/2008 du 7 mai 2008 émanant du comité sectoriel registre national », *R D.T.I.,* 2008, p. 413.
2. CPVP, avis n° 15/2006 du 14 juin 2006 relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrage des véhicules, n° 48.
3. CPVP, avis n° 02/97 du 8 janvier 1997 relatif au projet d'arrêté de la Région de Bruxelles-Capitale créant une banque de données concernant le personnel du ministère de la Région de Bruxelles-Capitale et des organismes d'intérêt public qui dépendent de la Région de Bruxelles-Capitale, p. 3, n° 5.
4. *Ibid.*, p. 3, n° 5.
5. CPVP, avis n° 07/2002 du 11 février 2002 relatif à un projet de loi créant la Banque-carrefour des entreprises, p. 6, n° 11.

Ainsi, on ne peut admettre le traitement des informations « nécessaires au service des caisses locales des dépôts et consignations ». Il faut utiliser un critère fonctionnel « répondant à la question de savoir pour quelle(s) finalité(s) le service des caisses locales des dépôts et consignations réalise des traitements de données à caractère personnel »[1].

d) Finalité de gestion administrative et finalité de contrôle. Enfin, il est recommandé de distinguer, parmi les finalités définies à partir d'un critère fonctionnel, les tâches de *gestion administrative*, d'une part, et les tâches de *contrôle*, d'autre part.

Selon nous, une telle distinction permet non seulement de perfectionner l'exigence de finalité, mais elle s'avérera également utile si l'on souhaite, à l'avenir, réutiliser les données. Cela facilitera le nécessaire examen de compatibilité entre la finalité poursuivie lors de la collecte initiale des données et celle poursuivie lors de leur réutilisation.

Par exemple, la CPVP[2] a approuvé le fait que, dans un avant-projet de loi relative à certains traitements de données à caractère personnel par le SPF Finances, le législateur ait indiqué que celui-ci ne peut utiliser les données à caractère personnel que dans la mesure de ce qui est nécessaire « a) aux opérations de gestion administrative pour l'établissement et la perception des impôts, taxes, droits et accises ; b) aux opérations de contrôle, de recouvrement et à celles liées à la gestion du contentieux des impôts, taxes, droits et accises […] »[3] effectuées par l'administration générale Impôts et Recouvrement.

14. Finalité explicite. Enfin, l'exigence d'une finalité explicite signifie que le législateur doit reprendre cette finalité textuellement dans la norme qui la définit, de manière à ce que cette finalité soit prévisible pour le citoyen. Cette finalité doit être exposée le plus clairement possible. Lorsque plusieurs finalités sont poursuivies par le traitement, une liste limitative de celles-ci doit figurer dans la norme. Citer quelques exemples de finalités possibles ne suffit donc pas[4].

En outre, la CPVP estime utile de faire figurer, dans la norme organisant le traitement des données à caractère personnel, non seulement la finalité poursuivie, mais également les finalités que ne peut poursuivre l'administration concernée. *A priori,* le recours à la « définition négative » de la finalité semble judicieux lorsqu'au vu des données utilisées ou de l'outil mis en place, on peut aisément craindre certains traitements qui ne respectent pas la *ratio legis* de la loi organisant le traitement. Néan-

1. CPVP, avis n° 01/2007 du 17 janvier 2007 concernant un avant-projet de loi relative à certains traitements de données à caractère personnel par le SPF Finances, p. 6, n° 27.
2. CPVP, avis n° 01/2007, *op. cit.,* p. 5, n° 21.
3. Avant-projet de loi relative à certains traitements de données à caractère personnel par le SPF Finances, *Doc. parl.,* Chambre, 2006-2007, n° 51-3064/001, p. 42.
4. Voy., notamment, CPVP, avis n° 42/2006, *op. cit.*, p. 7, n° 24.

moins, bien qu'elle ait le mérite de la clarté, la technique de la « définition négative » de la finalité risque d'affaiblir la portée de la « définition positive ». Ce faisant, ne risque-t-on pas d'utiliser des données pour réaliser certaines finalités qui n'ont pas été prévues par le législateur au motif que ce dernier ne les a pas interdites ? Il semble préférable de faire figurer les finalités qui ne peuvent être poursuivies dans l'exposé des motifs et de veiller à la précision de la finalité positive, particulièrement lorsque des données susceptibles d'un usage abusif sont en cause.

B. Le critère de proportionnalité

15. La notion. Le critère de proportionnalité est consacré à l'article 8, § 2, de la CEDH qui affirme que toute ingérence dans le droit à la protection de la vie privée doit être « nécessaire dans une société démocratique »[1].

Un traitement de données à caractère personnel proportionné respecte un juste équilibre entre, d'une part, l'ingérence dans la protection de la vie privée provoquée par ledit traitement et, d'autre part, l'objectif poursuivi par celui-ci. Dans l'e-gouvernement, l'objectif visé par un traitement de données est l'efficacité administrative.

En d'autres termes, le traitement de données doit être *approprié*. Cela signifie que la mesure doit être suffisamment énergique pour atteindre le but poursuivi. Par exemple, si l'objectif de la base de données « Registre national » est d'identifier chaque citoyen de manière unique, enregistrer leur nom et leur prénom ne suffit pas. Il faut davantage d'informations à propos de chaque individu, au risque de les confondre.

En outre, le traitement de données doit être *nécessaire*. Il faut veiller à ce qu'il n'existe pas une mesure moins liberticide que celle envisagée, qui permette d'atteindre le même objectif. Pour reprendre l'exemple du Registre national, il n'est pas nécessaire d'enregistrer l'état de santé de chaque citoyen pour l'identifier individuellement ni de savoir s'il a tenté de contracter un mariage de complaisance[2].

Le critère de proportionnalité s'applique tant au type de traitement mis en œuvre qu'aux données utilisées, comme on l'explique ci-dessous.

16. La proportionnalité du traitement. Dans la structure de l'administration en réseaux qui a été décrite précédemment, les données peuvent être collectées de deux manières différentes : soit de manière directe – ce que l'on appelle la collecte

1. Au sujet de l'exigence de proportionnalité dans la Convention européenne des droits de l'homme, voy. S. VAN DROOGHENBROECK, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux,* Bruxelles, Bruylant, Publication des Facultés universitaires Saint-Louis Bruxelles, 2001.
2. CPVP, avis n° 01/2009 du 14 janvier 2009 relatif à une demande d'avis concernant l'adaptation d'un code dans le type d'information relatif à l'état civil afin de prévenir les mariages de complaisance, n° 19.

directe des données –, soit de manière indirecte ce que l'on appelle la collecte indirecte de données. Ces deux types de collecte réalisent des équilibres différents.

La *collecte directe* de données consiste à obtenir les données directement de la personne concernée. Elle permet au citoyen de garder la maîtrise sur les informations qu'il livre à l'administration puisqu'il a connaissance de ce qu'il communique et qu'il livre une information exacte et à jour. Il peut également refuser de divulguer certaines informations, comme l'affirme la CPVP[1]. En pratique toutefois, cette possibilité de refus risque de se réduire à peau de chagrin. On imagine mal, en effet, un citoyen renoncer à une allocation ou à l'octroi d'un permis de bâtir au motif que l'information demandée est excessive.

La collecte directe de données souffre néanmoins d'inconvénients justifiant l'intérêt porté à la collecte indirecte de données dans le développement de l'e-gouvernement. À cet égard, un exemple français incite à la réflexion. Pour faciliter les démarches administratives des citoyens, un service public a été créé par une ordonnance de 2005[2], qui met à leur disposition un « espace de stockage accessible en ligne », ce que l'on pourrait appeler un « coffre-fort électronique ». L'usager peut y conserver les documents utiles à l'accomplissement de ses démarches et peut ainsi plus aisément les communiquer aux autorités administratives qui en ont besoin. Ce système est séduisant, car il facilite la communication d'informations aux administrations tout en permettant aux citoyens de garder la maîtrise sur celles-ci. Il faut néanmoins rester attentif au fait que le coffre-fort électronique réalise une centralisation d'un ensemble de données personnelles relatives à un même citoyen. En cas de faille de sécurité, un tiers pourrait y accéder. Par ailleurs, elle requiert du citoyen qu'il sache, d'une part, maîtriser l'usage d'Internet pour communiquer avec l'administration et, d'autre part, qu'il veille à répondre aux demandes des administrations.

La *collecte indirecte* de données consiste à obtenir l'information indirectement, c'est-à-dire à partir d'une base de données dans laquelle les informations ont été enregistrées au préalable. Ce type de collecte est encouragé dans la mise en place de l'e-gouvernement pour rendre effectif le principe de la collecte unique des données. Ainsi, plusieurs dispositions légales imposent désormais aux administrations de collecter indirectement les données déjà disponibles dans le réseau sectoriel dont elles font partie[3].

1. CPVP, avis n° 20/2008 du 11 juin 2008 concernant l'utilisation de données pour d'autres finalités que celles pour lesquelles elles ont été collectées initialement, p. 6, n° 19.
2. Article 7 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Voy., à ce sujet, M.-C. Roques-Bonnet, *Le droit peut-il ignorer la révolution numérique ?,* Paris, Michalon, 2010, p. 83.
3. À ce sujet, É. Degrave, « L'obligation de collecter les données à caractère personnel via la Banque-carrefour de la sécurité sociale : un renforcement de la responsabilité des institutions de sécurité sociale », *T.S.R.-R.D.S.*, 2014, pp. 525 à 557 ; É. Degrave, « L'intégrateur de service fédéral au cœur de la simplification administrative », *A.P.,* 2014, pp. 518 à 536.

Néanmoins, il présente des dangers pour la protection de la vie privée des citoyens, car ceux-ci perdent le contrôle de leurs informations. Entre autres risques, la CPVP a souligné que « des données collectées à des fins très différentes sont couplées, de sorte que de nouvelles données concernant la personne concernée apparaissent sans qu'elle n'ait un contrôle sur ce processus »[1].

Pour compenser la perte de contrôle du citoyen sur ses informations, il y a lieu d'offrir à celui-ci certaines garanties qui passent par la mise en place d'outils présentant, en eux-mêmes, des garanties de proportionnalité.

La source authentique de données et l'intégrateur de services offrent des solutions intéressantes pour organiser la circulation des données au sein de l'administration, à la condition de respecter certaines exigences.

La source authentique de données semble être un outil proportionné à l'objectif de fournir aux administrations des informations fiables sur les citoyens. Bien qu'elle constitue une menace pour la vie privée puisqu'elle a vocation à assurer la communication des données qu'elle contient, elle est entourée de garanties qui compensent l'immixtion créée dans la vie privée.

En effet, cette base de données d'un type particulier est conçue comme une source unique d'informations fiables. Pareille caractéristique est de nature à assurer un équilibre entre l'efficacité administrative et la protection de la vie privée. C'est pourquoi elle doit être préférée à la multiplication de bases de données au sein de chaque administration.

D'une part, grâce à la source authentique, les administrations savent aisément où trouver l'information de qualité nécessaire à l'exécution de leurs missions et ne doivent plus contacter la personne concernée. Elles ne doivent pas non plus s'assurer elles-mêmes de la mise à jour des données, celles-ci étant fiables. L'efficacité administrative est assurée.

D'autre part, en supprimant les copies de fichiers de données à caractère personnel, l'instauration d'une source authentique bénéficie également au citoyen. On évite le risque d'erreurs affectant les données qui se trouvent dans des copies de fichiers disséminées dans l'administration, celles-ci n'étant pas ou pas régulièrement mises à jour ou souffrant d'erreurs d'encodage. En outre, on diminue le risque d'accès illégitimes à ces données, puisqu'elles ne sont pas enregistrées à plusieurs endroits[2]. Ces garanties doivent être assurées par l'administration responsable de la source authentique. Ainsi, la protection de la vie privée est confortée.

1. CPVP, avis n° 20/2008 du 11 juin 2008 concernant l'utilisation de données pour d'autres finalités que celles pour lesquelles elles ont été collectées initialement, p. 6, n° 19.
2. En ce sens, voy. CPVP, recommandation 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public, p. 3.

Quant à l'intégrateur de services, dit aussi « banque-carrefour » ou « plate-forme d'échange d'informations », il répond adéquatement au souci d'organiser l'échange de données entre plusieurs administrations. Bien qu'il constitue une menace pour la protection de la vie privée, puisqu'il assure la circulation des informations, cet outil est conçu, lui aussi, pour réaliser un juste équilibre entre efficacité administrative et protection de la vie privée.

L'intégrateur de services améliore l'efficacité administrative. Grâce à lui, les informations recherchées sont rapidement acheminées vers l'administration demanderesse. De plus, en mettant en relation plusieurs sources authentiques, et en usant d'un portail Internet convivial, l'intégrateur de services permet aux administrations d'« obtenir des avantages équival[ant] à ceux d'un enregistrement de données centralisé sans que celui-ci ait effectivement lieu »[1].

Par exemple, l'application *Ebirth* témoigne de l'intérêt d'un intégrateur de services pour les administrations. *Ebirth* facilite l'échange des données relatives à la naissance d'un enfant. Ce service part du constat que tant les communes que la Communauté française et le SPF Économie ont besoin d'informations relatives à chaque naissance. Jadis, ces administrations obtenaient ces informations via des formulaires en papier envoyés par les hôpitaux. Aujourd'hui, les hôpitaux se connectent au portail *Ebirth*, encodent les données requises, et celles-ci sont acheminées respectivement vers les communes, la Communauté française et le SPF Économie, sans que ces institutions doivent accéder à une base de données qui reprendrait toutes les informations, y compris des données inutiles pour leurs missions respectives[2].

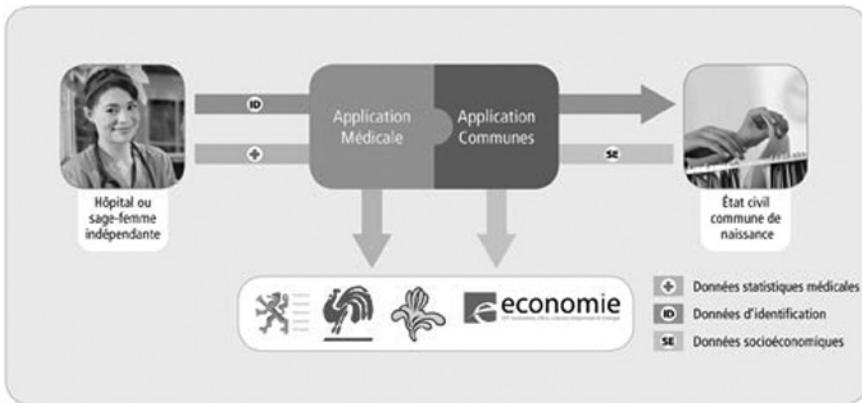


Illustration du service Ebirth*, disponible sur le site www.ehealth.fgov.be*

1. CPVP, recommandation n° 03/2009, *op. cit.*, p. 3, n° 7.
2. Pour plus d'informations sur *Ebirth,* voy. la présentation générale disponible sur www.ehealth.fgov.be, rubrique « Services en ligne », *Ebirth*.

L'intégrateur de services veille également au respect de la vie privée. Tout d'abord, cet outil permet aux administrations d'accéder à des données dont elles ne disposent pas, tout en assurant un enregistrement *décentralisé* des informations au sein des sources authentiques. On évite ainsi de centraliser les données dans une seule grande base de données à laquelle toutes les administrations auraient accès.

En cela, l'intégrateur de services est un outil mieux proportionné que l'intégrateur de données. Cette notion désigne une base de données qui réalise « l'agrégation de données à caractère personnel provenant de plusieurs sources authentiques et leur enregistrement dans une banque de données intégrées distincte, en vue de leur communication à des tiers »[1]. Comme l'a justement souligné la CPVP, un intégrateur de données représente un danger important pour la vie privée, car il s'agit d'une « concentration d'informations à un seul endroit. […] Il est évident qu'un incident de sécurité concernant une telle banque de données aura un impact bien plus important sur la vie privée qu'un incident concernant une des sources d'où les données ont été tirées »[2].

Il suffirait par exemple qu'un pirate informatique envoie, par Internet, un « cheval de Troie » à l'administration détenant la base de données centralisée pour parvenir à prendre possession de toutes les informations s'y trouvant. En outre, la concentration de données augmente le risque qu'un agent, cédant à la curiosité, consulte des données qu'il n'est pas autorisé à connaître dans le cadre de ses missions professionnelles.

Ensuite, l'intégrateur de services peut *contrôler* la légalité des accès demandés par les administrations.

C'est ce que fait la Banque-carrefour de la sécurité sociale en confrontant les demandes de données à la table des autorisations qui fait partie du répertoire des références, afin de s'assurer que l'administration demanderesse a reçu l'autorisation du comité sectoriel compétent pour les données demandées. À cet effet, comme l'a affirmé la CPVP, « travailler avec des répertoires de référence peut contribuer à éviter des consultations illicites »[3].

En cela, l'intégrateur de services est préférable à un système où chaque administration devrait identifier et consulter elle-même la source authentique de l'information recherchée.

Un tel système est pratiqué aux Pays-Bas, où il existe treize « basisregistraties » (parmi lesquels un registre « population », placé sous la responsabilité du ministère

1. CPVP, recommandation n° 03/2009, *op. cit.,* p. 2, n° 2.
2. *Ibid.,* p. 4, n° 10.
3. CPVP, recommandation n° 03/2009, *op. cit.,* p. 6, n° 17.

de l'Intérieur, un registre « entreprises », placé sous la responsabilité du ministère des Affaires économiques, un registre « adresses et bâtiments », placé sous la responsabilité du ministère de l'Infrastructure et de l'Environnement, etc.)[1]. Bien qu'un contrôle rigoureux de qualité des données soit organisé[2], l'inconvénient de ce modèle est de ne permettre qu'un contrôle *a posteriori* de la légalité de l'accès à l'information, par le « College Bescherming Gegevens ». Aucun organisme ne contrôle la communication de l'information avant qu'elle ait lieu.

Enfin, l'intégrateur de services peut également gérer un réseau primaire et un *réseau secondaire*. L'avantage d'un réseau secondaire est de pouvoir y placer des institutions fondées sur une base idéologique ou politique (telles que les mutuelles ou les syndicats). Ce faisant, l'administration demanderesse et l'intégrateur n'ont pas connaissance de l'institution auprès de laquelle sont conservées les données recherchées. L'intégrateur n'a connaissance que du réseau secondaire dans lequel se trouve la donnée recherchée, et est chargé de la demander à l'institution responsable de ce réseau secondaire.

17. La proportionnalité des données. Les données à caractère personnel faisant l'objet d'un traitement sont également soumises à l'exigence de proportionnalité. Elles doivent donc être limitées. Seules les données pertinentes et nécessaires peuvent être traitées.

Tout d'abord, l'administration ne peut collecter que des informations auxquelles elle a le droit d'accéder en vertu des normes en vigueur. C'est pourquoi il est conseillé de se demander si les informations dont l'utilisation est envisagée répondent à un « besoin réel »[3] de chaque administration. Il s'agit d'une application du principe de la spécialité des administrations. Celles-ci ne pourraient, à l'occasion d'un traitement de données, accéder à des informations qui ne sont pas nécessaires pour exercer leur mission.

Ensuite, les données utilisées doivent également être limitées au regard de la finalité poursuivie par le traitement de données. Dans certains cas, la communication d'une *mention « oui-non »* suffit pour permettre à l'administration d'exécuter ses missions. Ainsi, par exemple, lorsqu'une administration a besoin de connaître le revenu d'une

1. Pour de plus amples informations, voy. http://e-overheid.nl/onderwerpen/stelsel-van-basisregistraties/basisregistraties ; http://www.rijksoverheid.nl/onderwerpen/basisregistraties/overzicht-basisregistraties ; P. VAN DER MOLEN, « Authentic registers and good governance », FIG Working Week 2005, disponible à l'adresse http://www.fig.net/pub/cairo/papers/ts_01/ts01_04_vandermolen.pdf ; Y. ELLENKAMP et B. MAESSEN, « Napoleon's registration principles in present times : the Dutch system of key registers », 2009, disponible à l'adresse http://www.gsdi.org/gsdiconf/gsdi11/papers/pdf/101.pdf. Ces registres sont soumis à une loi du 9 juin 1994, dénommée « Wet gemeentelijke basisadministratie persoonsgegevens ». En raison de l'existence de cette loi, ces registres ne sont pas soumis à la loi sur la protection de la vie privée hollandaise (Wet bescherming persoonsgegevens, art. 2, d).
2. Pour un exemple, voy. le contrôle de la qualité des données du registre « adresses et bâtiments », Ministry of VROM, « Key registers of addresses and buildings », http://inspire.jrc.ec.europa.eu/ref_ser.cfm?id=32252.
3. Easi-Wal, *Formulaires. Guide pour les concevoir et les évaluer,* Namur, Commissariat wallon E-Administration et Simplification, coll. Guides pratiques, 2010, p. 7, disponible sur le site http://easi.wallonie.be/servlet/Repository/GPEasiWal_Formulaires.pdf?IDR=8632.

personne, la mention « oui-non » consiste à se demander s'il est nécessaire de communiquer à l'administration le montant exact du revenu de cette personne ou s'il lui suffit de savoir si la personne dépasse ou non le seuil requis par la législation pour obtenir l'avantage qu'elle réclame ou pour se voir imposer le paiement de la taxe à laquelle elle est soumise. Dans ce second cas de figure, l'administration émettrice communique un « oui » ou « non », qui est la réponse à la question « telle personne dépasse-t-elle tel seuil de revenu ? »

Par exemple, la Société flamande du logement social voulait obtenir, de la part du SPF Finances, le montant du revenu soumis à l'impôt des personnes physiques de certaines personnes souhaitant une aide pour se loger, tels les candidats emprunteurs d'un prêt social. Le comité sectoriel a constaté que, « pour entrer en ligne de compte pour un prêt social, une limite minimale et maximale de revenus est fixée »[1] et a affirmé que « le demandeur n'a […] pas besoin lui-même de toutes les données détaillées pour poursuivre dans ce contexte [ces] finalités […] mais doit généralement à ce stade uniquement pouvoir déterminer si les revenus de la personne concernée se situent ou non sous un certain seuil ». Dès lors, il a recommandé à cette institution « d'élaborer un système par lequel le demandeur ne reçoit une réponse qu'à la question de savoir si cette condition de revenus est respectée ou non. Ainsi, le demandeur n'a pas accès à toutes les données de revenus détaillées qui sont conservées au SPF Finances, ce qui donnerait évidemment lieu à un traitement de données plus proportionnel »[2].

Cette solution se répand de plus en plus. Elle est, par exemple, utilisée pour octroyer la réduction forfaitaire relative à la fourniture de gaz naturel, d'électricité et de mazout. Le SPF Économie n'accède pas à « un aperçu détaillé des revenus du demandeur », il « ne reçoit qu'une réponse positive ou négative à la question de savoir si le demandeur de la réduction répond ou non à la condition de revenus ». Ce faisant, il « ne reçoit pas d'autres données que celles strictement nécessaires »[3].

1. Délibération AF 14/2009, du 1er octobre 2009, relative à une demande d'autorisation de la « Vlaamse Maatschappij voor Sociaal Wonen (Société flamande du logement social) pour le traitement de données à caractère personnel enregistrées dans des banques de données du Service public fédéral Finances », p. 4, n° 10.
2. *Ibid.*, n° 24.
3. Délibération AF 11/2008, du 18 décembre 2008, relative à la transmission de données à caractère personnel du SPF Finances au SPF Économie, PME, Classes moyennes et Énergie, via la Banque-carrefour de la sécurité sociale, en vue de l'octroi d'une réduction forfaitaire pour la fourniture de gaz naturel, d'électricité et de mazout, p. 9, nos 28 et 29. Voy. également la délibération AF 08/2008, du 11 août 2008, relative à la transmission de données à caractère personnel du SPF Finances à la Banque-carrefour de la sécurité sociale et de la Banque-carrefour de la sécurité sociale au SPF Économie, PME, Classes moyennes et Énergie, en vue de l'octroi d'une réduction forfaitaire pour la livraison de gaz et d'électricité ; délibération AF n° 09/2008, *op. cit.*, n° 27.

IV. La transparence de l'e-gouvernement

18. Comment savoir ce que l'administration détient sur chaque individu et où se trouvent ces données dans l'administration ? La réponse à cette question intéresse notamment celui qui souhaite vérifier l'exactitude des données enregistrées à son sujet. Cette curiosité légitime est particulièrement importante dans la structure administrative nouvelle. En effet, puisque celle-ci est fondée sur la réutilisation maximale des données des citoyens, les éventuelles erreurs qui affectent ces informations risquent d'être reproduites à de multiples reprises. De plus, chaque individu doit être en mesure d'identifier les abus dans l'utilisation de ses données. Il est arrivé, par exemple, que des policiers repèrent de jolies conductrices et accèdent à leurs coordonnées en se connectant au registre de l'immatriculation des véhicules (DIV). Des personnes ont également été harcelées, car leur ex-conjoint avait pu repérer leur nouvelle adresse en accédant au Registre national. De telles utilisations des sources authentiques de données sont illégales, car elles ne poursuivent pas une finalité légitime. Il y a lieu de les sanctionner et, au préalable, de les identifier.

19. Le droit d'accès aux données. En vertu de l'article 10 de la loi du 8 décembre 1992, chaque personne a le droit d'accéder aux données qui la concernent et qui sont détenues par un responsable de traitement, telle une administration.

Ce droit permet à la personne qui l'exerce d'obtenir une vue assez précise de la manière dont ses propres données sont traitées par l'administration. En effet, le demandeur d'accès peut réclamer plusieurs types d'informations[1], que l'administration est alors obligée de lui fournir gratuitement. Ainsi, le citoyen peut demander si l'administration à qui il s'adresse traite des données à son sujet. Dans l'affirmative, il a le droit de savoir quelles données sont traitées, de connaître leur origine (où et comment elles ont obtenues), ainsi que les personnes à qui ces données ont déjà été communiquées et celles à qui elles seront éventuellement communiquées ultérieurement. Le citoyen peut également exiger d'être éclairé sur la logique qui sous-tend le traitement de ses données, lorsque la décision est entièrement automatisée[2]. Enfin, la réponse de l'administration doit mentionner l'existence des recours en opposition et en rectification et, le cas échéant, la possibilité de consulter le registre public. La

1. À cet égard, signalons que, pour faciliter la tâche du citoyen, la CPVP a établi une lettre type comprenant notamment la liste des types d'informations qui peuvent être demandées au responsable de traitement. Il revient au demandeur d'accès de cocher dans cette liste ce qu'il souhaite se voir communiquer. Cette lettre type est disponible sur le site Internet de la CPVP.
http://www.privacycommission.be/fr/exercice-droit-acces/vos-possibilites.
2. À ce sujet, voy. Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *L'application de la Convention 108 au mécanisme de profilage. Éléments de réflexion destinés au travail futur du Comité consultatif*. Rapport de J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever et A. Rouvroy, 11 janvier 2008, pp. 14 et 15, disponible sur le site http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profilage_2008_fr.pdf ; É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.,* n° 333.

demande doit être introduite par la personne concernée selon les formes prescrites par l'article 32 de l'arrêté royal du 13 février 2001.

Remarquons que l'administration doit répondre à la demande d'accès dans un délai de quarante-cinq jours ouvrables suivant la réception de la demande. Elle est également tenue de fournir ces informations sous une forme intelligible[1]. En d'autres termes, l'administration ne peut pas prétendre avoir communiqué les données traitées si elle s'est contentée d'envoyer un document reprenant, par exemple, une liste de codes censés représenter les types de données, alors que ceux-ci ne seraient pas traduits. Pour éclairer le citoyen sur l'origine des données, l'administration ne peut pas non plus, par exemple, se contenter de le renvoyer à un site Internet reprenant la liste des autorisations de comités sectoriels.

Le droit d'accès entend offrir au citoyen une maîtrise *a posteriori* de ses données, c'est-à-dire après que les données ont été collectées et traitées par l'administration. En prenant connaissance des traitements de données déjà effectués, le citoyen peut vérifier l'exactitude des informations utilisées et la légalité des traitements opérés. Le cas échéant, la personne concernée peut ensuite demander la rectification des données erronées, s'opposer à leur traitement ou réclamer l'interdiction de les conserver ou de les utiliser[2].

20. Le droit d'accès *in concreto* dans l'e-gouvernement. Le droit d'accès aux données personnelles manque manifestement d'effectivité. À titre indicatif, en 2012, l'INASTI, le SPF Finances et le Service public Wallonie n'avaient encore reçu aucune demande introduite en vertu de l'article 10, § 1er, de la loi du 8 décembre 1992[3].

Plusieurs éléments peuvent expliquer ce constat.

D'une part, ce droit d'accès aux données est généralement méconnu des citoyens, au même titre d'ailleurs que d'autres prérogatives organisées par la loi du 8 décembre 1992.

D'autre part, l'exercice de ce droit d'accès est laborieux. Il exige du citoyen qu'il ait une bonne connaissance de la structure et du fonctionnement de l'administration pour pouvoir identifier les institutions susceptibles de détenir des données à son sujet. Ensuite, la personne doit prendre la peine d'écrire à l'administration en apportant la preuve de son identité. Enfin, cette demande ne sera recevable qu'à la condition de ne pas se voir opposer une des nombreuses exceptions légales qui prévalent dans le secteur public[4].

1. Article 10, § 1er, de la loi du 8 décembre 1992.
2. Article 12 de la loi du 8 décembre 1992.
3. Entretien avec des agents des administrations concernées dans le courant de l'année 2013.
4. Voy. l'article 3, §§ 4, 5, 6, de la loi du 8 décembre 1992. Au sujet de ces exceptions au droit d'accès, voy. É. DEGRAVE, *E-gouvernement et protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, nos 336 et 337.

Par ailleurs, le droit d'accès aux données soulève également des difficultés pour l'administration saisie de la demande. Formuler une réponse satisfaisante peut représenter une charge de travail importante, singulièrement lorsque l'administration en question détient beaucoup de données au sujet de la personne concernée. Rappelons que l'administration doit non seulement communiquer les données détenues, mais également en préciser la finalité d'utilisation, les destinataires, les réutilisations envisagées, etc. La charge de travail est d'autant plus importante que la réponse de l'administration doit être formulée de manière intelligible, ce qui suppose des explications exhaustives présentées dans un langage clair.

Pour résoudre ces écueils, il peut être judicieux de faire appel à la technologie. Pour le moment, celle-ci est mise en œuvre principalement au bénéfice de l'administration qui voit ses tâches considérablement allégées par le développement des outils informatiques. Il est temps de développer davantage la technologie en faveur du citoyen cherchant à satisfaire sa curiosité légitime à l'égard de l'utilisation de ses données dans l'administration. Si tel n'est pas le cas, une rupture importante d'équilibre dans la relation entre l'administration et les individus risque de se créer[1]. En d'autres termes, « dans une démocratie, on ne peut exiger des citoyens qu'ils avancent à pied lorsque l'administration roule en limousine »[2].

Quelques outils aident déjà le citoyen à accéder à certaines de ses données au sein de l'administration. Malheureusement, actuellement, ils ne concernent que certaines administrations et demeurent peu connus du public. On pense notamment au répertoire de références de la Banque-carrefour de la sécurité sociale[3]. Cette base de données contient la localisation des types de données de chaque citoyen au sein du réseau de sécurité sociale. En contactant la Banque-carrefour de la sécurité sociale, le citoyen peut obtenir un extrait de son répertoire des références[4], qui lui permet d'identifier quelles sont les administrations détenant des données à son sujet et, le cas échéant, d'exercer auprès d'elles le droit d'accès organisé par l'article 10, § 2, de la loi du 8 décembre 1992.

Un outil très intéressant aussi est proposé par le site du Registre national[5]. En s'identifiant à l'aide de sa carte d'identité électronique, chacun peut visualiser les données enregistrées à son sujet dans le Registre national. Il est également possible, en cli-

1. À ce sujet, voy. É. DEGRAVE, *E-gouvernement et protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os^ 47 et s.
2. D.W. SCHARTUM, « Access to Government-held information : challenges and possibilities », *The Journal of Information, Law and Technology*, 1998/1, § 7.1 (traduction libre).
3. Pour de plus amples détails, voy. http://www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/about/mission/folder.html ; É. DEGRAVE, *E-gouvernement et protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os^ 25 et s.
4. Le répertoire des références est une base de données détenue par la Banque-carrefour de la sécurité sociale, contenant notamment une table « quoi-où » permettant de savoir quels sont les types de données enregistrés dans quelle administration. Pour plus d'informations, voy. notamment les explications fournies sur le site Internet de la Banque-carrefour de la sécurité sociale à l'adresse http://www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/about/mission/folder.html.
5. Voy. http://www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier/.

quant sur l'onglet « Historique des consultations », de vérifier quelle institution a consulté nos données dans les six derniers mois. Cette possibilité permet notamment d'identifier d'éventuels abus commis par des agents de l'administration dans l'utilisation des données à caractère personnel des citoyens.

Extrait d'un historique de consultations des données à caractère personnel du Registre national

La transparence de l'e-gouvernement gagnerait à ce que l'on développe les outils déjà existants et qu'on en organise d'autres, tels qu'un portail Internet dédié à la transparence de l'administration. Ce portail contiendrait un panorama général de la structure administrative. En y accédant, le citoyen devrait voir apparaître, notamment, la liste des administrations détenant une source authentique de données. Ensuite, en cliquant sur le nom de la source authentique, le type de données enregistrées par celle-ci devrait figurer sur l'écran. Enfin, en s'identifiant au moyen de sa carte d'identité électronique, le citoyen devrait pouvoir accéder, en ligne, aux données personnelles qui sont détenues à son sujet dans les sources authentiques de données de l'administration[1].

1. Pour de plus amples précisions à ce sujet, voy. É. DEGRAVE, *E-gouvernement et protection de la vie privée. Légalité, transparence et contrôle, op. cit.*, n^os 391 et s.

V. Le contrôle de l'e-gouvernement

21. Comment garantir au citoyen que l'administration respecte le droit et est sanctionnée si tel n'est pas le cas ? Le droit public organise des recours qui, s'ils sont exercés, sont efficaces. Ainsi, entre autres exemples, une loi qui organise un traitement de données à caractère personnel peut être annulée par la Cour constitutionnelle si elle porte atteinte au droit fondamental à la protection de la vie privée, consacré par l'article 22 de la Constitution. Une décision administrative peut être annulée par le Conseil d'État, section du contentieux administratif, s'il est établi qu'elle a été adoptée à partir de données que l'auteur de l'acte n'avait pas le droit d'utiliser. C'est le cas, par exemple, si le transfert de données n'a pas été autorisé par un comité sectoriel alors qu'il aurait dû l'être. Le Tribunal du travail peut mettre à néant la décision du CPAS qui refuserait le versement du revenu d'intégration sociale au motif que le demandeur n'aurait pas fourni certaines informations s'il est établi que le CPAS avait l'obligation de trouver ces informations par lui-même, via la Banque-carrefour de la sécurité sociale[1].

Malheureusement, ces recours souffrent de deux défauts majeurs. D'une part, en général, les citoyens ne les exercent pas. Bien souvent, ils n'ont pas connaissance des illégalités commises dans l'administration. Mais, au-delà, quand bien même ils les connaîtraient, il y a fort à parier qu'ils ne consacreraient pas du temps et de l'argent à contester ces problèmes qui les dépassent largement. D'autre part, quand ces illégalités sont effectivement attaquées, on constate que les avocats n'invoquent pas ou invoquent mal les règles de protection des données. Certains arrêts laissent ainsi apparaître que des arguments tirés de la protection des données n'ont pas été invoqués alors qu'ils auraient pu être porteurs.

A. La Commission de la protection de la vie privée

22. Un rôle essentiel. Le régime juridique de la protection des données organise d'autres moyens d'action, davantage adaptés à l'univers technologique. En particulier, la CPVP joue un rôle essentiel. Elle dispose de moyens d'action intéressants dans le contexte de l'e-gouvernement. À l'image du Médiateur fédéral, la CPVP reçoit les plaintes des citoyens lorsqu'elles touchent à la protection de la vie privée. Une médiation peut ensuite être organisée entre la personne concernée et l'institution visée. D'autres moyens d'action sont à sa disposition, tels que le droit d'intenter une action judiciaire dans l'intérêt collectif[2]. Les traitements de données illégaux

1. Pour un cas de jurisprudence, voy. notamment C. trav. Bruxelles (8e ch.), 21 avril 2010, R.G. n° 2008/AB/51591 et n° 2009/AB/51809.
2. Voy. l'article 32 de la loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel.

commis dans l'administration peuvent ainsi être dénoncés en justice par l'autorité de protection des données.

Néanmoins, à certains égards, le contrôle exercé par la CPVP manque d'efficacité et d'effectivité. Par exemple, cette institution n'a encore jamais exercé l'action judiciaire dans l'intérêt collectif. Ce recours reste d'ailleurs assez méconnu. Pour permettre à la CPVP d'agir plus efficacement, il serait judicieux d'augmenter ses moyens humains et de lui conférer plus de moyens d'action, tels qu'un pouvoir d'admonestation et un pouvoir d'amende, comme en dispose déjà son homologue français, la Commission nationale de l'informatique et des libertés (« CNIL »).

23. Les comités sectoriels, organes de la CPVP. De plus en plus souvent, les données des citoyens qui sont collectées et enregistrées par certaines administrations sont ensuite réclamées par d'autres administrations, voire par des sociétés privées. Par exemple, il est intéressant, pour un CPAS, d'obtenir de Famifed[1] le montant d'allocations familiales versé à un allocataire social afin de calculer le montant de l'allocation à laquelle il a droit, sans devoir demander cette information à l'allocataire en question. Il est tentant, pour certaines sociétés privées, d'enregistrer une copie du numéro d'identification au Registre national des consommateurs afin de pouvoir identifier ces personnes de manière unique dans leur base de données, etc.

Depuis quelques années, de tels transferts de données doivent être autorisés par la CPVP. Plus précisément, depuis une réforme législative intervenue en 2003, la CPVP comprend, en son sein, des organes dénommés « comités sectoriels », chargés d'autoriser, ou non, la communication des données enregistrées dans les bases de données de l'administration fédérale[2]. Il existe actuellement six comités sectoriels, chacun étant compétent en fonction de la nature des données qu'il contrôle.

Ainsi, le *comité sectoriel du Registre national* est compétent pour octroyer « l'autorisation d'accéder aux informations [enregistrées dans le Registre national] »[3] ainsi que « l'autorisation d'utiliser le numéro d'identification du Registre national »[4].

Le *comité sectoriel de la Banque-carrefour des entreprises* est compétent pour autoriser l'accès aux données de la Banque-carrefour des entreprises[5].

Le *comité sectoriel de la sécurité sociale et de la santé* est divisé en deux sections : la section « sécurité sociale » et la section « santé ». La section « sécurité sociale » est compétente, en somme, pour contrôler les traitements de données effectués par

1. Famifed est l'Agence fédérale pour les allocations familiales, jadis appelée l'Office national d'allocations familiales pour travailleurs salariés.
2. Article 31*bis* de la loi du 8 décembre 1992.
3. Article 5 de loi du 8 août 1983 sur le Registre national. Voy. également l'article 15 de cette même loi.
4. *Ibid.,* articles 8 et 15.
5. Articles 17 et 18, § 2, du 16 janvier 2003 portant création d'une Banque-carrefour des entreprises, *M.B.,* 5 février 2003.

les institutions de sécurité sociale[1]. Par ailleurs, la section « santé » veille à la légalité des traitements de données à caractère personnel relatives à la santé, au sens de la loi du 8 décembre 1992[2].

Le *comité de surveillance sectoriel « Phénix »* contrôle les traitements de données issues de la banque de données Phénix[3], qui est la banque de données de l'ordre judiciaire.

Le *comité de surveillance « Statistique »* est compétent pour autoriser l'Institut national de statistique à communiquer des données d'étude codées[4].

Enfin, le *comité sectoriel pour l'Autorité fédérale* a une compétence résiduelle, en ce qu'il est compétent pour autoriser « toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, […] à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel créé au sein de la Commission pour la protection de la vie privée »[5].

Ces comités sectoriels ont été créés pour que la légalité des transferts de données soit contrôlée au cas par cas et par des spécialistes du secteur dans lequel les échanges de données ont lieu. C'est l'idée que des personnes du terrain peuvent ainsi veiller à ce que les traitements de données accomplis dans l'administration respectent tant la loi que les préoccupations concrètes de l'administration. Comme l'a affirmé la CPVP pour souligner l'intérêt des comités sectoriels, « ces organes de contrôle spécifiques […] dans lesquels siégeraient, entre autres, des représentants du secteur concerné, devraient s'attacher à rechercher des solutions concrètes à

1. Ce terme doit être compris au sens de l'article 2, 2°, de la loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale. Voy. également l'article 43*bis,* alinéa 1er, de cette loi.
2. Article 43*bis,* alinéa 2, de la loi du 15 janvier 1990 relative à la Banque-carrefour de la sécurité sociale. Voy. également l'article 42, § 2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, *M.B.,* 22 décembre 2006. Ainsi sont soumis à l'autorisation de la section « sécurité sociale », et non à celle de la section « santé », les traitements de données à caractère personnel relatives à la santé, au sens de la loi du 8 décembre 1992, par les institutions de sécurité sociale et les personnes visées à l'article 18 de la loi du 15 janvier 1990 (art. 15, § 2, 2°, et art. 43*bis* de la loi du 15 janvier 1990) ; les traitements de données sociales à caractère personnel relatives à la santé (au sens de la loi du 15 janvier 1990) par les instances d'octroi visées à l'article 11*bis* de la loi du 15 janvier 1990 (art. 43*bis* de la loi du 15 janvier 1990) et les traitements de données sociales à caractère personnel relatives à la santé par une instance de sécurité sociale vers une autre instance de sécurité sociale, une instance d'octroi visée à l'article 11*bis* de la loi du 15 janvier 1990 ou une personne visée à l'article 18 de la loi du 15 janvier 1990 (art. 15, § 1er, de la loi du 15 janvier 1990). Sur la question de la compétence d'autorisation de chaque section de ce comité sectoriel, voy. également CPVP, avis n° 43/2006 du 8 novembre 2006 relatif au projet de loi portant dispositions diverses – Création d'un comité sectoriel de la sécurité sociale et de la santé, p. 7, n° 15.
3. Articles 22 et s. de la loi du 10 août 2005 instituant le système d'information Phénix, *M.B.,* 1er septembre 2005.
4. Article 17 de la loi du 22 mars 2006 modifiant la loi du 4 juillet 1962 relative à la statistique publique et la loi du 8 août 1983 sur le Registre national. Les données d'étude sont « les informations qui serviront à établir des résultats statistiques ». On les dit « codées » lorsqu'elles « ne peuvent être mises en relation avec une personne identifiée que par l'intermédiaire d'un code » [art. 3 de la loi du 22 mars 2006 modifiant la loi du 4 juillet 1962 relative à la statistique publique et la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.,* 21 avril 2006. Signalons que cette disposition n'est pas encore entrée en vigueur].
5. Article 36*bis* de la loi du 8 décembre 1992.

des problèmes concrets » et « exercer un contrôle “de première ligne” dans le domaine de la protection des données à caractère personnel »[1].

24. La CPVP : une autorité administrative ? Le statut de la CPVP soulève de multiples interrogations. Entre autres questions, cette institution est-elle une autorité administrative ? Dans la négative, ses décisions ne seraient pas attaquables devant le Conseil d'État, section du contentieux administratif, ce qui pose maintes difficultés dans un État de droit.

À première vue, la CPVP ne peut pas être qualifiée d'autorité administrative, car elle ne répond pas à l'ensemble des critères d'une telle autorité. En effet, bien qu'elle soit instituée par le législateur, qu'elle exerce une mission d'intérêt général et qu'elle puisse prendre des décisions obligatoires à l'égard des tiers, la CPVP n'est pas soumise à un réel contrôle des pouvoirs publics[2].

Néanmoins, à notre sens, ce n'est pas pour autant qu'il faille renoncer à soumettre les décisions de la CPVP au contrôle de la section du contentieux administratif du Conseil d'État. Plusieurs solutions existent[3]. Parmi celles-ci, celle de la « qualification par assimilation » retient notre attention dans ces lignes. Il s'agit d'une technique d'interprétation que pourrait appliquer le Conseil d'État pour accepter de connaître des recours introduits contre les décisions de la CPVP. Cette technique se définit comme une « fiction juridique [qui] consiste […] à rattacher délibérément à une catégorie juridique un objet qui, aux yeux de l'observateur avisé, ne remplit pas les conditions traditionnellement nécessaires pour y entrer, de façon à permettre la mise en œuvre des conséquences attachées à cette catégorie »[4]. Cette technique de qualification se fonde sur un raisonnement par analogie.

En l'occurrence, supposons que le Conseil d'État estime que la CPVP ne répond pas aux conditions nécessaires pour entrer dans la catégorie juridique de l'autorité administrative. On constate cependant que la CPVP « ne présente pas de différence fondamentale »[5] avec les institutions traditionnellement qualifiées d'« autorité administrative ». En effet, ainsi qu'on l'a dit, la CPVP répond à trois des quatre critères de l'autorité administrative. C'est pourquoi on applique à la CPVP le régime juridique applicable aux autorités administratives. Cette assimilation ne se fonde pas sur une identité réelle entre la CPVP et les institutions traditionnellement qualifiées

1. CPVP, avis n° 30/96 du 13 novembre 1996 relatif à un avant-projet de loi adaptant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à la directive 95/45/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, n° 60.
2. Voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle, op. cit.,* pp. 600 et s.
3. *Ibid.*, pp. 680 et s.
4. C. Vautrot-Schwarz, *La qualification juridique en droit administratif,* Paris, L.G.D.J., 2009, pp. 432 et 433. Voy. également D. De Roy, « Établissements publics, organismes d'intérêt public et *tutti quanti* : la qualification juridique des satellites de l'administration », note sous Cass., 19 mars 2010, *R.C.J.B.,* 2013, pp. 88 et s.
5. C. Vautrot-Schwarz, *op. cit.,* 2009, p. 435.

d'autorités administratives. Elle se justifie par une identité de raison juridique : le but que l'on poursuit en soumettant les décisions des autorités administratives au contrôle du Conseil d'État est similaire à celui qui justifie le contrôle des décisions de la CPVP.

Plus particulièrement, s'agissant de la question de savoir si le Conseil d'État est compétent pour se prononcer sur la légalité d'une décision de la CPVP, on pourrait raisonner comme suit. Le Conseil d'État a été institué « en tant que juridiction spécifique en vue d'offrir une protection juridictionnelle supplémentaire à celle des cours et tribunaux contre les actes administratifs entachés d'illégalité »[1]. Cette juridiction œuvre donc à la protection des citoyens à l'égard des décisions arbitraires qui s'appliqueraient à eux[2].

Or les décisions de la CPVP s'apparentent en de nombreux aspects aux décisions émanant d'une autorité administrative. Les personnes soumises à une décision illégale de la CPVP pourraient subir le même dommage que les individus visés par une décision illégale émanant d'une autorité administrative. La CPVP doit donc pouvoir être rattachée à la catégorie juridique de l'autorité administrative, afin que chaque personne visée par une décision de la CPVP puisse soumettre celle-ci à l'examen du Conseil d'État et ne pas avoir à subir les conséquences néfastes d'une décision entachée d'illégalité.

25. La CPVP : une autorité indépendante ? La CPVP doit exercer ses moyens d'action en toute indépendance, comme le lui imposent la loi du 8 décembre 1992[3] et les normes supranationales qui régissent la matière[4].

a) L'exigence d'indépendance. Selon la Cour de justice de l'Union européenne, l'exigence d'indépendance imposée aux autorités de protection des données s'explique par le souci de permettre à ces autorités d'être en mesure d'effectuer un examen objectif et impartial de l'équilibre à atteindre entre la circulation des données à caractère personnel et la protection de la vie privée des personnes concernées. Cette affirmation de la Cour de justice de l'Union européenne résulte d'une interprétation téléologique de la directive 95/46 à laquelle elle s'est prêtée dans deux arrêts récents. Le premier arrêt concerne les autorités de protection des données instituées dans les *Länder* allemands[5], tandis que le second vise l'autorité de protection des données autrichiennes[6].

1. C.C., 15 mai 1996, n° 31/96, B.2.1.
2. E. Maron, « Les notions d'acte administratif et d'autorité administrative : compétence ou incompétence du Conseil d'État pour connaître des recours en annulation dirigés contre les actes de nature administrative accomplis par des autorités relevant du pouvoir législatif ou du pouvoir judiciaire ? », *in Le Conseil d'État de Belgique. Cinquante ans après sa création (1946 à 1996),* Bruxelles, Bruylant, 1999, p. 328.
3. Article 23 de la loi du 8 décembre 1992.
4. Articles 28 de la directive 95/46 et 1.3 du Protocole additionnel à la Convention n° 108.
5. C.J.U.E. (Gr. Ch.), 9 mars 2010, *République fédérale d'Allemagne c. Commission,* C-518/07.
6. C.J.U.E. (Gr. Ch.), 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10.

Plus précisément, la Cour rappelle que l'objectif poursuivi par la directive européenne est d'assurer la libre circulation des données entre les États membres. Puisque ces échanges d'informations peuvent heurter la vie privée des citoyens concernés, les autorités de contrôle doivent être des « gardiennes [des] droits et libertés fondamentaux »[1]. Leur tâche revient à « assurer un juste équilibre entre, d'une part, le respect du droit fondamental à la vie privée et, d'autre part, les intérêts qui commandent une libre circulation des données à caractère personnel »[2]. Partant de là, l'indépendance des autorités de contrôle s'entend des garanties permettant à ces institutions d'examiner cet équilibre « de manière objective et impartiale »[3].

De quelle sphère d'influence cherche-t-on à protéger les autorités de protection des données par cette exigence d'indépendance ?

Rappelons que les autorités de protection des données sont chargées de protéger le droit fondamental à la vie privée dans le secteur des traitements de données à caractère personnel. Leur intervention peut également avoir un impact économique en favorisant la concurrence loyale entre des opérateurs privés désireux d'utiliser des données à caractère personnel[4]. Les traitements de données étant effectués au sein du secteur privé et du secteur public, ces autorités contrôlent donc un grand nombre d'organismes.

Dès lors, s'agissant de la CPVP, celle-ci est à la fois un relais de l'action étatique, lorsqu'elle contrôle le secteur privé, et un moyen de contrôle de l'État, s'agissant de l'examen de traitements de données effectués par les administrations[5]. Le contrôle exercé par les comités sectoriels vise même principalement les administrations puisqu'ils peuvent empêcher une administration de communiquer les données qu'elle détient. C'est pourquoi, compte tenu du fait que l'autorité de protection des données doit faire preuve d'objectivité et d'impartialité tant à l'égard des sociétés privées que de l'administration, il y a lieu de lui assurer une indépendance particulièrement ample.

L'interprétation que donne la Cour de justice de l'Union européenne de l'exigence d'indépendance confirme ce propos. En effet, la Cour soutient qu'étant donné que la directive 95/46 prescrit à l'autorité de protection des données d'agir en « toute » indépendance, cela signifie qu'elle doit « jouir d'une indépendance qui [lui] permette

1. C.J.U.E. (Gr. Ch.), 9 mars 2010, *République fédérale d'Allemagne c. Commission,* C-518/07, § 23.
2. *Ibid.,* § 24.
3. *Ibid.*, § 25. Dans le même sens, C.J.U.E. (Gr. Ch.), 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10, §§ 40 et 41.
4. À ce sujet, voy. É. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles », obs. sous Bruxelles (9e ch.), 9 mai 2012, *J.T.,* 2012, pp. 691 à 693. Dans la décision commentée, la Cour d'appel de Bruxelles condamne une société privée qui utilise des données à caractère personnel en violant une interdiction d'un comité sectoriel. Le juge considère qu'il s'agit d'une illégalité, source de concurrence déloyale.
5. E. Debaets, « Les autorités administratives indépendantes et le principe démocratique : recherches sur le concept d'"indépendance" », Rapport présenté au VIIIe Congrès mondial de l'Association internationale de droit constitutionnel, Mexico, 6-10 décembre 2010, disponible sur le site www.juridicas.unam.mx/wccl/ponencias/14/254.pdf.

d'exercer [ses] missions sans influence extérieure ». Cela exclut « non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel »[1]. En d'autres termes, l'autorité de protection des données doit faire preuve d'une indépendance objective et subjective. Objectivement, cette autorité doit être organisée de manière telle qu'elle soit « au-dessus de tout soupçon de partialité »[2]. Subjectivement, il importe qu'aucun risque d'influence politique ne crée auprès des membres de l'autorité de protection des données une « obéissance anticipée »[3].

Concrètement, la Cour de justice de l'Union européenne en déduit que l'autorité de protection des données ne peut pas être soumise à un contrôle de tutelle de l'État[4]. La Cour juge également que l'exigence d'indépendance s'oppose à ce que tout ou partie des membres de l'autorité de protection des données soient des fonctionnaires soumis au contrôle de l'État[5].

b) L'indépendance de la CPVP. L'indépendance de la CPVP pose question au regard du mode de désignation de ses membres et de la manière dont elle est composée.

Les membres de la CPVP sont élus par la Chambre des représentants sur des listes comprenant, pour chaque mandat à pourvoir, deux candidats présentés par le Conseil des ministres[6].

Dans son rapport sur les autorités chargées de la protection des données à caractère personnel, l'Agence des droits fondamentaux de l'Union européenne fait apparaître que l'élection des membres de l'autorité de protection des données par le Parlement – pratiquée également en Grèce, en Allemagne et en Slovénie – est un mécanisme de désignation bien plus respectueux de l'exigence d'indépendance que la nomination par le gouvernement – comme en Irlande ou au Luxembourg – ou le rattachement de ladite autorité au ministère de la Justice – comme au Danemark ou en Lettonie et comme c'était le cas en Belgique avant 2003[7].

L'élection des membres de la CPVP par la Chambre des représentants n'est donc pas, en soi, une atteinte à l'indépendance de l'autorité de protection des données.

1. C.J.U.E. (Gr. Ch.), 9 mars 2010, *République fédérale d'Allemagne c. Commission,* C-518/07, § 30 ; C.J.U.E. (Gr. Ch.), 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10, § 41.
2. *Ibidem*.
3. *Idem*.
4. *Ibidem*.
5. C.J.U.E. (Gr. Ch.), 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10, § 66.
6. Article 24, § 1er, de la loi du 8 décembre 1992.
7. European Union Agency for Fundamental Rights, 2010, pp. 19 et 20.

Néanmoins, la présentation des candidats par le Conseil des ministres pose question, puisque le pouvoir du Conseil des ministres de présenter deux candidats pour chaque poste à pourvoir limite le choix de la Chambre des représentants, en le teintant d'une logique majoritaire. La section de législation du Conseil d'État affirme ainsi que ce pouvoir est « inhabituel » et est « de nature à limiter sérieusement le choix des chambres législatives »[1].

En outre, on peut raisonnablement penser que, concrètement, les candidats choisis par le Conseil des ministres émanent des cabinets ministériels et des administrations. Une fois membres de la CPVP, ces personnes sont appelées à contrôler l'action administrative. N'y a-t-il pas là un risque de manque d'impartialité dans l'exercice de leurs tâches[2] ? C'est en ce sens, en tout cas, que se prononce la section de législation du Conseil d'État. Constatant qu'« un grand nombre de responsables des traitements sont des autorités publiques dépendant du pouvoir exécutif », elle soutient que « ce droit exclusif de présentation conféré au pouvoir exécutif et la logique majoritaire qui le sous-tend ne sont pas en parfaite harmonie avec la nature des missions [de la Commission] »[3]. Rappelons également que cette situation pose question au regard de la position de la Cour de justice de l'Union européenne, pour qui l'exigence d'indépendance impose que les membres de l'autorité de protection des données doivent exercer leur fonction en dehors de toute influence extérieure, qu'elle soit directe ou indirecte. Enfin, l'Agence des droits fondamentaux de l'Union européenne émet une crainte semblable. Elle cite la Belgique comme un des États dans lesquels la procédure de désignation des membres de l'autorité de protection des données implique l'intervention de l'exécutif, du législatif et du judiciaire, et ne manque pas de préciser : « [I]t is essential to ensure that the Government does not, in practice, control directly or indirectly the majority of the appointees, thus effectively frustrating the purpose of a pluralistic nomination procedure »[4].

Pour remédier à ces écueils, il pourrait être judicieux que les membres de la CPVP ou, au moins, une partie de ceux-ci puissent être élus sans être présentés par le Conseil des ministres[5]. Les candidats à un poste de membre de la CPVP pourraient

1. SLCE du 28 novembre 1990 sur un projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. parl.,* Chambre, 1990-1991, 1610/1, p. 61.
2. Dans le même sens, voy. F. KAUFF-GAZIN, « Vers une conception européenne de l'indépendance des autorités de régulation ? », *Europe,* 2010, p. 15. Cette auteure affirme que « la nomination des membres de l'autorité par le gouvernement […] peut poser problème au regard de l'indépendance effective et concrète des membres. Une fois nommés, il n'est pas sûr que les membres concernés s'affranchissent totalement d'une proximité ou d'une "sensibilité" gouvernementale ».
3. SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Doc. parl.,* Chambre, 1997-1998, n° 1566/1, p. 240.
4. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Data protection in the European Union : the Role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II,* 2010, pp. 19 et 20.
5. En ce sens : SLCE du 28 novembre 1990 sur un projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. parl.,* Chambre, 1990-1991, n° 1610/1, p. 61 ; SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Doc. parl.,* Chambre, 1997-1998, n° 1566/1, p. 240.

se présenter devant la Chambre afin d'y exposer les raisons de leur motivation. S'ensuivrait un débat public avant l'élection, par les parlementaires, du meilleur candidat. Par ailleurs, la légitimité des membres de la CPVP élus pourrait être renforcée en prévoyant un vote à majorité spéciale, et non simple, à la Chambre. Ce faisant, les candidats devraient convaincre un plus grand nombre de parlementaires, ce qui renforcerait la voix de l'opposition dans le débat et, dans le même temps, transcenderait la division de la Chambre en groupes linguistiques. Cette idée s'inscrit dans la lignée de la section de législation du Conseil d'État qui a affirmé qu'« il serait souhaitable, en raison des missions confiées à la CPVP, que l'opposition parlementaire soit associée au processus de désignation des membres de la Commission »[1].

Une telle solution est appliquée en Grèce, par exemple, où les membres de l'autorité chargée de la protection des données sont désignés par le Parlement après une procédure qui requiert un consentement entre la majorité et l'opposition[2]. Au-delà des frontières européennes, cette solution est également appliquée au Québec, où les membres de la Commission d'accès à l'information sont nommés par l'Assemblée nationale qui doit approuver leur nomination par un vote d'au moins deux tiers de ses membres[3].

On peut également s'interroger sur l'indépendance de la CPVP au regard de sa composition. Celle-ci est marquée par un pluralisme des intérêts représentés et un souci d'expertise des membres. Ainsi, siègent au sein de la Commission, au moins un juriste, au moins un magistrat, ainsi que plusieurs experts, à savoir au moins un informaticien, un spécialiste de la gestion des données dans le secteur public et un spécialiste de la gestion des données dans le secteur privé.

Quant aux comités sectoriels institués au sein de la CPVP, ils sont composés, pour moitié, de membres de la CPVP et, pour moitié, de membres externes désignés en fonction de leur expertise[4]. La désignation d'« assesseurs externes spécialisés » est présentée comme un « gage de compétence et d'efficacité »[5], tandis que la présence des membres de la CPVP au sein de chaque comité sectoriel se justifie par le souci d'unifier les solutions avancées en matière de protection des données à caractère personnel.

1. SLCE du 28 novembre 1990 sur un projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. parl.,* Chambre, 1990-1991, n° 1610/1, p. 61.
2. Article 16.2 de la loi 2472/1997 on the *Protection of individuals with regard to the processing of personal data* disponible sur le site de l'Autorité de protection des données hellénique http://www.dpa.gr.
3. Article 104 de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.
4. Article 31*bis,* § 2, de la loi du 8 décembre 1992 et article 3 de l'arrêté royal du 17 décembre 2003 précité. La composition du comité sectoriel de la sécurité sociale et de la santé fait exception à cette règle, conformément à l'article 37 de la loi du 15 janvier 1990 précitée.
5. Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *Doc. parl.,* Chambre, 2002-2003, n° 50-1940/001, p. 12.

Sans remettre en question le pluralisme et l'expertise de la CPVP, des questions se posent quant à l'objectivité et l'impartialité de certains membres. En effet, la loi du 8 décembre 1992 n'empêche pas que le fonctionnaire d'une administration soumise au contrôle de la CPVP soit également membre de cette Commission. La loi encourage même cette situation, en exigeant la présence, au sein de la CPVP, d'un spécialiste de la gestion des données dans le secteur public et en prévoyant que le Conseil des ministres présente les candidats, ce qui peut favoriser les membres issus de l'administration, comme expliqué plus haut. Dans cette hypothèse, ledit membre est à la fois le contrôleur et le contrôlé, ce qui sème le doute sur son impartialité.

Ce problème est d'autant plus important que certaines personnes sont à la fois membres de la CPVP et membres d'un ou plusieurs comités sectoriels. La loi du 8 décembre 1992 impose, en effet, que la moitié des membres d'un comité sectoriel émanent de la CPVP. Le problème du « contrôleur contrôlé » s'étend alors à plusieurs organes.

Pour remédier à ce problème, deux solutions pourraient être envisagées.

Une première solution serait de maintenir une composition collégiale de la CPVP à la condition de renforcer l'indépendance de chaque membre désigné. À cet égard, la solution française est intéressante. L'objectivité et l'impartialité de la CNIL sont organisées au travers d'une composition pluraliste qui vise à concilier les intérêts de personnes venant d'horizons distincts. Ainsi, la CNIL comprend quatre parlementaires (deux députés, deux sénateurs), six hauts magistrats (deux conseillers d'État, deux conseillers à la Cour de cassation et deux conseillers à la Cour des comptes), ainsi que deux membres du Conseil économique, social et environnemental. Ces douze membres sont élus par l'assemblée ou la juridiction dont ils émanent. S'ajoutent à ces membres cinq personnalités qualifiées, dont une est désignée par le président de l'Assemblée nationale, une par le Président du Sénat et trois par décret.

En outre, des incompatibilités de mandats devraient être prévues par la loi. Ainsi serait-il préférable d'instaurer une incompatibilité entre l'exercice d'un mandat de membre de la CPVP et/ou d'un comité sectoriel, et un poste de directeur d'une administration.

Une deuxième solution serait de désigner une personne qui présente elle-même suffisamment de garanties d'expertise, d'objectivité et d'impartialité dans ce domaine, sans exclure qu'elle puisse s'entourer d'une équipe de conseillers. Cette personne serait élue par la Chambre des représentants, au terme d'un examen et d'une audition. Elle incarnerait la protection de la vie privée face à l'opinion publique.

Plusieurs autorités de protection des données sont organisées de cette manière. Tel est le cas, notamment, en Suisse[1], en Allemagne[2] et au Canada[3].

Enfin, l'indépendance institutionnelle de la CPVP s'apprécie au regard des ressources mises à sa disposition et de la possibilité d'adopter des décisions à l'abri d'ordres ou d'injonctions provenant de l'extérieur.

La CPVP était instituée dans un premier temps auprès du ministre de la Justice. Pour lui assurer davantage d'indépendance à l'égard de l'exécutif, une importante réforme législative intervenue en 2003 a placé la CPVP sous l'égide de la Chambre des représentants[4]. Aujourd'hui, la CPVP ne fait donc plus partie du pouvoir exécutif.

Désormais, le budget de la CPVP est fixé par la Chambre des représentants, tout comme les règles applicables à son secrétariat. Au-delà, la CPVP exerce sa mission de manière indépendante. En effet, la Chambre des représentants ne dispose que du droit de voir communiquer le rapport d'activités de la CPVP, ainsi que son règlement d'ordre intérieur, sans, toutefois, pouvoir modifier ce dernier.

L'indépendance institutionnelle de la CPVP semble donc renforcée par ce rattachement à la Chambre des représentants, dans la mesure où aucun contrôle de tutelle ne peut orienter les agissements de l'autorité de protection des données.

B. Le détaché à la protection des données

26. Bientôt une obligation. Selon la directive 95/46[5], le détaché à la protection des données est la « personne désignée par le responsable du traitement de données [qui] s'assure que les traitements effectués ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées […] [qui est] employée ou

1. En Suisse, les missions de l'Autorité de protection des données sont exercées par le Préposé fédéral à la protection des données et à la transparence. Ce dernier est rattaché administrativement à la Chancellerie fédérale. Il est aidé par un secrétariat permanent ainsi que trois unités regroupant plusieurs personnes. Deux de ces unités sont compétentes pour des questions de protection des données, tandis que la troisième se charge de la transparence (art. 26 et s. de la Loi fédérale sur la protection des données du 19 juin 1992).
2. En Allemagne, le *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* est nommé par le gouvernement fédéral pour une durée de cinq ans renouvelable une fois. Comme le Préposé fédéral à la protection des données et à la transparence en Suisse, le Commissaire à la protection des données allemand est entouré d'une équipe structurée en différents départements en fonction des matières traitées (*Bundesdatenschutzgesetz*, § 22 ; http://www.bfdi.bund.de/EN/FederalDataProtectionCommissioner/StructureAndTasks/organisation_node.html).
3. Le Commissariat à la protection de la vie privée du Canada est également organisé de cette manière. Il est composé d'une Commissaire, qui a la qualité de haute fonctionnaire du Parlement. Elle est entourée d'une Commissaire adjointe et d'un Comité consultatif externe composé d'une vingtaine de personnes spécialisées dans la protection de la vie privée et issues de différents milieux (universités, entreprises privées, administrations, magistrature, etc.). (Sur la Commissaire à la protection de la vie privée du Canada, voy. http://www.priv.gc.ca/au-ans/bio_f.asp ; sur la Commissaire adjointe à la protection de la vie privée du Canada, voy. http://www.priv.gc.ca/au-ans/bio_cb_f.asp.)
4. Loi du 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la CPVP, *M.B.,* 26 juin 2003.
5. Considérant 49 et article 18 de la directive 95/46.

non du responsable du traitement de données, [et] doit être en mesure d'exercer ses fonctions en toute indépendance »[1].

Pour l'heure, instituer un détaché à la protection des données est une possibilité laissée à chaque institution qui traite des données à caractère personnel. Le futur règlement européen en matière de protection des données à caractère personnel en fait une obligation dans l'administration. On peut s'en réjouir, car la désignation d'un détaché à la protection des données présente de nombreux avantages pour l'administration.

27. Une fonction trop peu développée en Belgique. Malheureusement, en Belgique, le rôle de détaché à la protection des données n'a pas encore reçu l'attention qu'il mérite.

Actuellement, le législateur n'impose pas qu'un détaché à la protection des données soit présent dans chaque organisme traitant des données à caractère personnel. Tout au plus, la loi du 8 décembre 1992 cite-t-elle le « préposé à la protection des données »[2] en guise d'exemple de mesure particulière de protection à l'égard des « traitements présentant des risques particuliers au regard des droits et des libertés des personnes concernées »[3].

Certes, la loi du 15 janvier 1990 prévoit l'obligation, pour toute institution de sécurité sociale, de désigner un « conseiller en sécurité ». Néanmoins, ce rôle n'est pas à confondre avec celui de détaché à la protection des données. Comme l'affirme la CPVP, la notion de détaché à la protection des données « indique, en effet, que la mission de cette personne est plus large que celle de veiller à la sécurité des données, y compris l'intégrité et la disponibilité, mais comprend aussi le devoir "d'assurer, d'une manière indépendante, l'application de la [loi du 8 décembre 1992] ainsi que de ses mesures d'exécution", ce qui signifie outre les missions de sécurité, celle du contrôle du respect des principes de légitimité, de proportionnalité et du droit d'accès des personnes concernées »[4].

1. Considérant 49 de la directive 95/46. Voy. également l'article 18 de la directive 95/46.
2. Dans un souci de clarté, la section de législation du Conseil d'État avait recommandé de reprendre, dans la loi belge, les termes « détaché à la protection des données », utilisés par la directive 95/46 [voy. SLCE, avis du 2 février 1998 sur un avant-projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *op. cit.*, 1997-1998, n° 1566/1, p. 233]. Cela n'a pourtant pas été fait. Quoi qu'il en soit, les notions de « détaché à la protection des données » et de « préposé à la protection des données » désignent la même fonction.
3. Article 17*bis* de la loi du 8 décembre 1992. Pour un cas d'application de cette disposition, voy. CPVP, avis n° 27/2007 du 4 juillet 2007 sur un projet d'arrêté royal précisant les règles relatives au traitement des listes négatives.
4. CPVP, avis n° 19/2002 du 10 juin 2002 relatif à un projet de la loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, à un projet d'arrêté royal relatif aux cartes d'identité, à un projet d'arrêté royal portant mesures transitoires en ce qui concerne la carte d'identité électronique en Belgique, p. 11, n° 22.

En n'organisant pas d'obligation de recourir à un détaché à la protection des données, la Belgique se distingue de l'Allemagne, qui rend obligatoire la présence d'un détaché à la protection des données dans les organismes du secteur public, au niveau fédéral et dans certains états[1].

La Belgique se distingue également de la Suisse, qui impose un détaché à la protection des données dans les institutions fédérales[2].

Cette obligation existe également en dehors des frontières européennes. Ainsi, au Québec, il y a, dans chaque organisme public, une « personne responsable de la protection des renseignements personnels »[3], chargée notamment de tenir le registre de toutes les communications de renseignements effectuées par l'organisme émetteur[4], d'organiser les ententes de partage avec les autres administrations[5], etc. Ce responsable est « la personne ayant la plus haute autorité au sein [de l']organisme public »[6]. Celle-ci peut toutefois « désigner comme responsable un membre de l'organisme public ou de son conseil d'administration […] ou un membre de son personnel de direction » à qui il peut « déléguer tout ou partie de ses fonctions »[7].

Plus encore, ni le législateur ni le Roi n'ont défini le statut du détaché à la protection des données. La loi du 8 décembre 1992 se contente de renvoyer au Roi le soin de déterminer le statut du détaché à la protection des données, ce qui n'a jamais été fait. Dès lors, aucune garantie n'est établie pour assurer l'indépendance du détaché à la protection des données.

28. Les encouragements de la section de législation du Conseil d'État. Cette lacune suscite des critiques de la part de la section de législation du Conseil d'État, qui insiste sur la nécessité que le législateur fixe le statut des détachés à la protection des données « en vue de garantir au mieux leur indépendance, parce qu'on ne peut totalement exclure que leur situation, notamment leur appartenance aux institutions où les traitements ont lieu, ne mette cette indépendance en péril »[8]. Il s'agit là d'un point qui doit être réglé par le pouvoir législatif, et non le pouvoir exécutif, en vertu de l'article 22, alinéa 2, de la Constitution et du principe de légalité y consacré. La section de législation du Conseil d'État affirme que, si « le législateur n'[est] pas en

1. Article 4f (1) de la *Bundesdatenschutzgesetz*. Pour un commentaire de ce régime, voy. N. MÉTALLINOS, « La fonction de "détaché à la protection des données" en Allemagne et aux Pays-Bas », *Dr. soc.*, n° 12, 2004, p. 1068.
2. Article 23 de l'ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993.
3. Article 8 de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.
4. Article 67.3 de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.
5. Article 64 de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.
6. Article 8 de la loi québécoise sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chapitre A-2.1.
7. Idem.
8. SLCE, avis du 2 février 1998 sur un avant-projet de loi « transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *Doc. parl.,* Chambre, 1997-1998, n° 1566/1, p. 232.

mesure de déterminer, dès à présent, dans l'avant-projet de loi, quelles seront les garanties de cette indépendance effective, par l'énoncé de règles précises, le concept […] doit être abandonné ; en effet, confier au Roi, comme le fait très indirectement le projet, le soin de régler la matière, ne se conçoit pas, en raison de l'article 22, alinéa 2, de la Constitution, et parce qu'il serait anormal que le pouvoir exécutif trace les contours de cette indépendance, alors qu'il n'est pas exclu que celui-ci désigne en son sein des délégués, en sa qualité de responsable de nombreux traitements visés par la loi »[1].

29. Les encouragements de la CPVP. La CPVP critique également l'absence de statut légal du détaché à la protection des données[2]. Elle tente néanmoins de pallier ce silence en apportant quelque éclairage à ce sujet. Elle livre des critères pour garantir effectivement cette indépendance, faisant écho à des législations étrangères.

La CPVP affirme ainsi que l'indépendance du détaché à la protection des données signifie notamment qu'il doit pouvoir initier des projets ou en refuser, *sans pression extérieure*[3]. En outre, l'exercice des missions confiées au détaché à la protection des données ne peut lui causer des *désavantages*, tel qu'un licenciement ou une réaffectation à un autre poste[4]. C'est particulièrement important lorsque la législation prévoit la possibilité, pour le détaché à la protection des données, d'alerter l'autorité nationale de contrôle en matière de protection des données d'une pratique illégale au sein de son institution, comme c'est le cas en France[5]. En d'autres termes, le détaché à la protection des données ne doit pas craindre un licenciement s'il est contraint de dénoncer des pratiques illégales au sein de l'institution qui l'a engagé. Or la peur d'entrer en conflit avec la direction de l'institution pourrait mettre en cause l'indépendance du détaché à la protection des données. Il semble donc nécessaire que cette personne jouisse d'un statut de salarié protégé, comme c'est le cas en Allemagne où

1. SLCE, avis du 2 février 1998 sur un avant-projet de loi « transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *op. cit.*, 1997-1998, n° 1566/1, p. 232.
2. CPVP, avis n° 15/2002 du 2 mai 2002 relatif à un projet d'arrêté royal portant exécution de l'article 3, § 6, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, n° 17 ; CPVP, avis n° 35/2012 du 21 novembre 2012 sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, n° 128.
3. Voy., notamment, CPVP, avis n° 39/2008 relatif au projet d'arrêté royal relatif à l'accès des personnes désignées de l'Office des étrangers aux faits concrets de police judiciaire et aux informations relatives aux groupements et aux personnes traitées dans le cadre des missions de police administrative et centralisées dans la banque de données Nationale générale, visée à l'article 44/4 de la loi du 5 août 1992 sur la fonction de police, n° 31.
4. Idem.
5. L'article 51 du décret du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit que « la Commission nationale de l'informatique et des libertés peut être saisie à tout moment par le correspondant à la protection des données à caractère personnel ou le responsable des traitements de toute difficulté rencontrée à l'occasion de l'exercice des missions du correspondant. L'auteur de la saisine doit justifier qu'il en a préalablement informé, selon le cas, le correspondant ou le responsable des traitements.
La Commission nationale de l'informatique et des libertés peut à tout moment solliciter les observations du correspondant à la protection des données ou celles du responsable des traitements ».

les détachés à la protection des données ne peuvent être licenciés par l'employeur que pour des raisons importantes[1].

Enfin, pour garantir cette indépendance, la CPVP conseille de placer le détaché à la protection des données à un *niveau de hiérarchie* « tel qu'il ait la possibilité de communiquer directement avec le management/comité de direction et d'exercer sa mission directement auprès du responsable de traitement »[2].

1. L'article 4f, § 3, de la *Bundesdatenschutzgesetz* prévoit que la nomination au poste de détaché à la protection des données peut être annulée en application du paragraphe 626 du *Bürgerliches Gesetzbuch* (C. civ. allemand) qui prévoit que des raisons importantes doivent être établies pour mettre fin au contrat ; C. KLUG, « Improving self-regulation trough (law-based) corporate data protection officials », disponible sur le site de l'Association des détachés à la protection des données allemande, www.gdd.de.
2. Idem.